Privacy Impact Assessment

MRP Amazon Web Services General Support System (MRP AWS GSS)

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date September, 2022
- Prepared for: Marketing and Regulatory Programs

United States Department of Agriculture

Privacy Impact Assessment for the

MRP AWS GSS

September, 2022

<u>Contact Point</u>
Abhai Singh
USDA APHIS MRP

<u>Reviewing Official</u>
Tonya Woods
Director, Freedom of Information and Privacy Act Staff
United States Department of Agriculture

Abstract

- The Marketing Regulatory Programs Amazon Web Services General Support System (MRP AWS GSS) and its components, the Palantir Platform and the Veterinary Services Data Integration Services (DIS), have combined and are being assessed and authorized under a single accreditation boundary.
- Within the MRP AWS GSS, the VS DIS utilizes the Palantir Platform to integrate data from existing Agency systems including:
  - Emergency Management Response Services 2.0 (EMRS2)
  - VMAC (VS Multisystem on Azure Cloud) child applications:
    - Animal Disease Traceability Information System (ADTIS)
    - Laboratory Messaging Services (LMS)
    - Veterinary Services Laboratory Submissions (VSLS)
    - Veterinary Services Process Streamlining (VSPS)
  - Surveillance Collaboration Services (SCS)
  - VS Searchable Test Result Application for NVSL Diagnostics (STRAND)
  - User Management System (UMS)
  - Mi-Corporation Mobile Data Collection (MiCo)
  - User Fee System (UFS)
  - Veterinary Export Health Certification System(VEHCS)

Overview

The Marketing and Regulatory Programs mission of the USDA is to provide administrative and technical resources to the Agricultural Marketing Service (AMS) and Animal and Plant Health Inspection Service (APHIS) mission area agencies. This PIA is created for the MRP Amazon Web Services General Support System (MRP AWS GSS), which provides a cloud platform for agencies that wish to take advantage of AWS GovCloud services.

The Palantir Platform and VS Data Integration Services (VS DIS) are components of the MRP AWS GSS. VS DIS utilizes the Palantir Platform to view, analyze, transform, aggregate, and model data. It is a secure platform where data and code can be versioned for quality control and users can collaborate to answer organizational questions without sacrificing security or data integrity. Data pipelines, analyses, and reports can be shared and discovered and be managed by access controls, thereby eliminating the creation of data management work performed in local, ungoverned silos. VS will also use the Palantir platform for data entry and the uploading of files into data pipelines managed in Palantir.

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?

SCS: The following information from SCS may be shared with the Palantir component of the MRP AWS GSS.

- Employee – USDA APHIS VS SCS maintains name, address, phone and personal identification number (professional license number, Veterinary Accreditation number, regulatory official ID) information for USDA and State animal health employees directly involved in disease program activities.

- Other – USDA APHIS VS SCS maintains name, address, and phone information for individuals identified as contacts for premises (locations) and owners of animals or animal related operations involved with the various animal disease/pest surveillance and or control programs that could be identified in agency assigned miscellaneous numbers (case numbers, flock IDs, laboratory accessions, and permit numbers.) and personal identification number (professional license number, Veterinary Accreditation number) information for private veterinarians. Because of the varying nature of the premises, including sole proprietorships, and the undocumented relationship of the contact to the premises, many of the contacts are simply private citizens deserving of protection under the Privacy Act.

VSLS: The following information from VSLS may be shared with the Palantir component of the MRP AWS GSS.

The information in the VSLS may contain the following information types: Name, address, contact telephone, e-mail address for collectors, submitters and herd/flock owners, or associated APHIS personnel (Scrapie Epidemiologist), latitude/longitude coordinates, operation type(s), species and breeds, national premise identification number or state location identifier number, flock or herd identification numbers, characteristics of the animal or specimen collected, testing an test results. VSLS can also be used to monitor the dates and times between sample collection and results entry, and the database maintains an audit of the users that created and/or updated collection information or results in the underlying database.

VSISM: The following information from VSISM may be shared with the Palantir component of the MRP AWS GSS.

The information in the VSISM may contain the following information types: Name, address, contact telephone, e-mail address for collectors, submitters and herd/flock owners, or associated APHIS personnel, latitude/longitude coordinates, operation type(s), species and breeds, national premise identification number or state location identifier number, flock or herd identification numbers, characteristics of the animal or specimen collected, testing an test results. VSISM maintains an audit of the users that created and/or updated collection information.

EMRS2: The following information from EMRS2 may be shared with the Palantir component of the MRP AWS GSS.

Information includes name; address (including city), county, state, postal code, latitude/longitude coordinates; premises identification number; and telephone number. The EMRS2 may also contain the name and telephone number of the person(s) who provided the initial report concerning the premises, and the name, telephone number, and e-mail address of the person responsible for the investigation of the premises. EMRS2 also contains information about APHIS employees who may be deployed as members of Incident Command System (ICS) teams and their position assignment.

LMS: The following information from LMS may be shared with the Palantir component of the MRP AWS GSS.

Test results for multiple diseases including Avian Influenza, Swine Enteric Coronavirus Disease, Vesicular Stomatitus Virus, Swine Influenza Virus, African Swine Fever, Foot Mouth Disease, and others are transmitted over secure http in an HL7 message, or loaded by spreadsheet by federal users. Rhapsody messaging services is the current endpoint for external messaging and performs authentication as well as schema validation before accepting messages. Some surveillance analysts currently have read only access to the SQL Server repository data for analysis and reporting, but the preferred avenue is through DIS.

VSPS: The following information from VSPS may be shared with the Palantir component of the MRP AWS GSS.

The VSPS system collects information from veterinarians who apply on-line to become federally accredited, from importers that are requesting a permit to import animals, and from accredited veterinarians that are submitting health certificates for the export and interstate movement of animals.

VS personnel processes and approve applications for federal accreditation, document actions taken against accredited veterinarians, process permit requests and issue import permits, maintain the animal import rules, process export health certificates, and maintain the export protocols. State personnel issue permits for interstate movement requests and maintain the state protocols.

ADTIS: The following information from ATDIS may be shared with the Palantir component of the MRP AWS GSS.

General contact information is recorded in the Standardized Premises Information System (SPIS) on individuals that are associated with a premises; specifically, name, address, company name, contact numbers, and e-mail. All other information is in regards to the animals in the possession of the customers and only collected during a disease or other health event. Such animal information collected includes: specific systems that provided the information (i.e., premises data, animal ID manufacturers, and animal tracking institutions), Premises ID, Animal ID, date of event, event type, breed and sex.

The information contained in the system is based on the tracing of animals. Personal information of individuals is only used for verification and contact purposes for the goal of tracing and containment of diseased or exposed animals.

STRAND: The following information from STRAND may be shared with the Palantir component of the MRP AWS GSS.

Customer:

- Submitters of Diagnostic Samples
    - Shipping Address
    - Invoice Address
    - Contact Name
    - Contact Phone Number
    - Contact e-mail

US Government Employee:

- Employee Information
    - Employee Name
    - Employee E-mail

Diagnostic sample information

- Wildlife/ Zoo/ owner
- If owner then:
    - Owner Name
    - Owner City
    - Owner State
    - Owner Zip
    - Owner Country
-
- Collected by
- Authorized by
- Preservation
- Purpose
- s

Slaughtering Establishment Information:

- Establishment ID
- Establishment Name

- Establishment Address
- Establishment City
- Establishment State
- Establishment Zip
- Establishment Country

Tuberculosis Sample Information:

- Food Inspector Name
- Veterinarian Name
- Market Buyer Name

UMS: The following information from UMS may be shared with the Palantir component of the MRP AWS GSS.

The UMS system contains information on state and federal employees regarding their roles and permissions for MRP applications and systems, which includes employee first and last name, middle initial, eAuth username, eAuth email, mobile and office phone number.

MiCo: The following information from MiCo may be shared with the Palantir component of the MRP AWS GSS.

The MiCo platform enables VS to create electronic forms to support animal surveillance and traceability programs and functions. MiCo forms collect information on state and federal employees using the application, which includes their roles and permissions for MiCo, employee first and last name, middle initial, eAuth username, eAuth email, and can include premises-relevant information, such as premises owner name, email, phone number, and premises address.

UFS: The following information from UFS may be shared with the Palantir component of the MRP AWS GSS.

The UFS system contains financial records and information on state and federal employees, private citizens, and businesses, such as first and last name, associated email address, phone and fax numbers, address, UFS usernames, and comments associated with the user's account.

VEHCS: The following information from VEHCS may be shared with the Palantir component of the MRP AWS GSS.

The VEHCS system contains animal/animal-related export records and information on state and federal employees, private citizens, and businesses, such as first and last name, associated email address, phone and fax numbers, address, type of export, location of export, VEHCS username, and also ties the export data to financial records in UFS.

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

Information in this system comes primarily from the operational VS information systems: Surveillance Collaboration Services (SCS), Veterinary Services Laboratory Submissions (VSLS), Emergency Management Response Services 2.0 (EMRS2), Laboratory Messaging Services (LMS), Animal Disease and Traceability Information System (ADTIS), VS Searchable Test Result Application for NVSL Diagnostics (STRAND), VS Integrated Surveillance Modules (VSISM), User Management System (UMS), Mi-Corporation Mobile Data Collection (MiCo), User Fee System (UFS), Veterinary Export Health Certification System (VEHCS), spreadsheet uploads from APHIS employees, and external partners. No data is collected directly from the user.

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

PII information is collected as part of a core component of the VS operational activities and part of the comprehensive operations and integrated on-farm surveillance and outbreak response in order to achieve the VS mission to maintain and promote the health and availability of animals, animal products and veterinary dynamics. This integrated data is being used by VS programs to manage and perform functions and operations related to disease monitoring, surveillance, animal disease traceability, import/export functions, and reporting (e.g. tracing and containment of diseased or exposed animals). In addition they are used for prevention, detection and early response to outbreaks. Collected PII enables implementation and operations for VS operational activities relating to tracing and attribution of data. Beyond enabling VS operations, PII is generally not shared externally. The only time PII is shared externally is to fulfill FOIA requests.

1.4 How is the information collected?

The Palantir Platform primarily collects information stored and entered into other systems. It includes a database containing information ingested on a routine or ad hoc basis from other government/USDA databases, commercial and public source data providers to which USDA employees have access. Routine ingests of data from the sources listed, occur by means of an automated data ingestion process. Palantir software periodically scans the source database to detect additions, modifications, or deletions to the records contained in the source system. The Palantir database is then updated to reflect these changes. Ad hoc ingests of data occur either by users entering data or importing electronic files into the system via a data import application. The source of ad hoc ingests varies depending on the circumstances, but may include a particular user's knowledge, manual queries of other databases, reference materials, or other open source data. The Palantir system generates the index, tables, and analytical results described in Question 2.1 using the source data.

1.5 How will the information be checked for accuracy?

Palantir only assists the human evaluation and decision-making processes associated with data retrieved from other systems. Therefore, Palantir relies on the system(s) and/or program(s) performing the original collection to provide accurate data. In addition, APHIS-VS governance processes take advantage of Palantir capabilities to improve quality of data that is integrated and interfaced as the VS DIS.

VS DIS users refer to a variety of data sources available through the system and other systems to verify and correlate the available information to the greatest extent possible. Where incorrect information is identified, it is corrected either in VS DIS or in the source system, which then pushes the corrected data to VS DIS. The accuracy of APHIS-owned data, state data, commercial (SNOMED and LOINC codes) and public source data (National Agriculture Statistics Service, National Animal Health Laboratory Network reference data, MAPBOX) is dependent on the original source.

The Palantir index in the relational database is updated frequently – according to business needs. As the source system data is corrected, the data in Palantir will be automatically updated and corrected as well. This automated data update process helps to ensure the data in the VS DIS is as current and accurate as possible.

The Palantir Platform also implements automated data validation rules / checks such as missing data and invalid data entry. Additionally, VS/MRP-IT technical SMEs can implement validation rules / data checks programmatically with automated alerts for success / failure as appropriate.

For ad hoc data uploads, in the event uploaded data is later identified as inaccurate, VS DIS users are required to modify their own ad hoc uploads to correct the data. If the user who uploaded the data no longer has access privileges to VS DIS, it is the responsibility of a supervisor or systems administrator to make the appropriate changes to the incorrect data. VS DIS users are trained how to modify ad hoc data for accuracy and correctness in the system.

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

- The Animal Damage Control Act of 1931, 7 U.S.C. 8301 et seq. of the Animal Health Protection Act
- The Animal Health Protection Act, 7 U. S. C. 8301-8317
- 7 USC Sec. 7629
- 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 Homeland Security Presidential Directive 9.
- Farm Bill as approved by Congress
- Title 9, Code of Federal Regulations (9 CFR)
- 21 U.S.C. 105, 111-114a-1, 116, 125, 134b, 134f

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

Unauthorized disclosure of employee and other personal data, as identified in Section 1.1 above, was the primary privacy risk identified in the PIA. USDA APHIS Program staff and leadership are all responsible for protecting the privacy rights of the employees and other persons identified in the MRP AWS GSS and its components (the Palantir Platform and VS DIS) as required by applicable State and Federal laws. Specific mitigation activities are:

- All access to the data in the system is controlled by formal authorization. Each individual’s supervisor must identify (authorize) what functional roles that individual needs in the MRP AWS GSS and its components. Additionally, each quarter users with access are randomly sampled and their supervisors must reaffirm access (MRP-IT UMS).
- Access to the Palantir Platform and VS DIS is controlled by the USDA eAuthentication system and/or USDA VPN.
- The application limits access to relevant information and prevents access to unauthorized information.
- All users receive formal system training and are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training.
- At the login screen of the application the warning banner must be acknowledged before users are allowed access.

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 Palantir Platform and VS DIS allows VS to have a global view of the information that is collected to support the mission of VS. The uses of the information will mirror that in the original source systems in addition to integrated reporting to allow for leadership view and decision making. VS DIS allows for a comprehensive view of all the data and creates efficiency across the organizations within one tool with the same epi, surveillance response, emergency, and import/export activities.

The following data is used from VSLS:
Collection site information including premises address and contact information, flock/herd owner and samples collected are entered in the application by Federal employees and cooperating State employees based on information on forms. Test results are entered in the application generally by state personnel working in one of the NAHLN laboratories around the country.

In exceptional reporting support cases, such as for the current Scrapie SCS system, APHIS surveillance business analysts have been allowed to produce reports against the VSLS database directly using their Business Intelligence (BI) tools, until reporting can be developed against the management repository.

The following data is used from VSISM:
The information collected from states, users, individuals and/or businesses in the general public is collected on OMB approved form VS 10-4, 6-35, 10-12 and 5-38 at a minimum, as well as approved non-forms.

The following data is used from LMS:

The information collected includes: name, address information, business information and laboratory operations information, laboratory identification, laboratory location, test results, patient (animal) information, communication integrity information.

The following data is used from EMRS2:
The system collects, uses and maintains information such as:

> Owner or operator of the premises where the animals subject to investigation are located; the system includes the following information, such as, but not limited to, the name; address (including city, county, State, postal code, and latitude/longitude coordinates); premises identification number; and telephone number.

Referring contact information, which includes name and telephone number.

Case coordinator of the premises investigation; the system includes name, telephone number, and email address.

APHIS employees; the system includes the following information, such as, but not limited to the name; agency, program, and group; current duty assignment; encrypted employee identification number; grade, series, and step; duty city and State; home address, including latitude/longitude coordinates; home telephone number; home email address; emergency contact information; work and field addresses, email addresses and telephone numbers; and supervisor contact information.

The following data is used from VSPS:

The VSPS system collects information from veterinarians that apply on-line to become federally accredited, from importers that are requesting to import animals, and from accredited veterinarians that are creating Interstate Certificates of Veterinary Inspection (CVIs). Accredited veterinarians can also create the Equine Infectious Anemia (VS 10-11) form and submit it electronically to a lab for the lab to enter results which then creates an official form.

VS personnel processes and approve applications for federal accreditation, document actions taken against accredited veterinarians, create the animal importation requests for animal movements into the US, create and manage reservations at the import quarantine centers, and maintain the product export and product import facilities and inspections.

State personnel can manage the State certification statements for their State for Interstate movements. States can also view all health certificates that have been Issued by Accredited veterinarians that have an Origin or Destination of their State. They can review and approve or reject each health certificate. States also can enter paper certificates into the Retro-CVI section of the Interstate module.

Data is entered into VSPS by the users and forms can then be created and printed if needed from the data entered.

The data is maintained in the system database kept on the Azure cloud. Users update the data in the system as needed.

The following data is used from ADTIS:

General contact information is recorded in the ADTIS Landing Page and Premises on individuals that are associated with a premises; specifically, name, address where the animals are located and premises contact addresses, company name, contact numbers, and e-mail. All other information pertains to the animals in the possession of the customers and is only collected during a disease or other health event. Such animal information collected includes specific systems that provided the information (i.e., premises data, animal ID manufacturers, and animal tracking institutions), Premises ID, Animal ID, date of event, event type, breed and sex.

The information contained in the system is based on the tracing of animals. Personal information of individuals is only used for verification and contact purposes for the goal of tracing and containment of diseased or exposed animals.

PINs for premises are linkable to the animal owner. This information is only disseminated to the animal owner. The reporting of premise data is also disseminated. It includes contact information from the PM record and event reporting by PIN from AIMS. No other dissemination of PII occurs from the ADTIS.

The following data is used from STRAND:

Customer:

- Submitters of Diagnostic Samples
    - Contact Name
    - Contact Phone Number
    - Contact e-mail

US Government Employee:

- Employee Information
    - Employee Name
    - Employee Job Title
    - Employee Business Phone no.
    - Employee E-mail
    - Employee Supervisor
    - Employee Organizational Group within NVSL and Center for Veterinary Biologics (CVB)

Diagnostic sample information

- Wildlife/ Zoo/ owner
- If owner then:
    - Owner Name
    - Owner City
    - Owner State
    - Owner Zip
    - Owner Country
- Collected by
- Authorized by

Tuberculosis Sample Information:

- Food Inspector Name
- Veterinarian Name

- Market Buyer Name
- Market Buyer Address

.

<u>The following data is used from UMS:</u>

The UMS platform is maintained by MRP-IT and controls user access and rights to VS applications, e.g. grants authorization for specific data types and actions with that data. DIS pulls in user information and associated DIS permissions from UMS to control user access to data and rights for operations with said data, as well as authorization to participate in specific workflows, within DIS. Examples of controlled user access include visibility of surveillance data resources, and row-level access to resources by state. Beyond controlling user permissions, UMS user data is not used for any additional purpose within DIS.

<u>The following data is used from MiCo:</u>

The data collected from the MiCo platform currently include Federally Approved Livestock Market Agreements (as defined in 9 CFR 71.20) and surveillance data associated with ASF-CSF submissions. DIS pulls the Livestock Market Agreement records into the platform and unions the data to historic records for records / data management purposes. PII on the Livestock Market Agreement electronic records is stripped through a programmatic process until it aligns with a pre-existing standard of publicly available information on the Agreements. After data processing, the Livestock Market Agreements are published to a public Tableau dashboard to support reporting.

The ASF-CSF submissions are pulled into DIS and integrated into an existing pipeline which combines all streams of surveillance data on ASF-CSF. The records are used to support ASF-CSF surveillance and reporting to VS internal and external stakeholders.

<u>The following data is used from UFS:</u>

Financial records are pulled into DIS to support budgetary reporting to VS internal stakeholders including the Office of the Deputy Administrator. UFS data are also utilized to support in-platform workflows and data aggregations, e.g. integration of UFS data into VEHCS to support filtering and searchability of VEHCS data.

<u>The following data is used from VEHCS:</u>

The data in VEHCS are used to support tracking of Export certificates and reporting. Currently, export certificate data pulled into DIS are being used in a manner that will streamline the physical and data management activities associated with certification generation and approval of live animal and animal product exports.

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

VS DIS uses the capabilities of the Palantir Platform to perform analysis on the integrated data, including on the database layer backend and on the semantic layer frontend (end-user facing). Other business analysis tools such as Alteryx and Tableau may be used. Statistical modeling and analysis may be performed using Python, R, SAS or another statistical software, and GIS tools such as ARCGIS may be used to geographically represent the data. Other USDA and APHIS MRP approved data analysis tools may be used. Any data outlined in Section 1.2 above could be included as outputs. Data outputs may include figures, graphs, tables, and maps in the form of manuscripts, reports, and presentations. Data may also be provided in other formats as needed for operational activities.

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

VS DIS may use data that is publicly available in order to standardize reference tables in order to facilitate the analysis of clinical information. Publicly available data from the Veterinary Terminology Services Laboratory (VTSL) may be used in order to apply standardized medical terminology. VS DIS may also use publicly available data obtained from the Food and Agricultural Organization (FAO), World Organization for Animal Health (OIE) and Dairy Herd Improvement Association (DHIA). All data obtained in this manner will exclude PII.

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.

- Privacy rights of the employees and other persons will be protected by USDA APHIS management within the limits of the Privacy Act of 1974. MRP AWS GSS and its components have security controls to address access/security of information.
- All access to the data in the system is controlled by formal authorization. Each individual’s supervisor must identify (authorize) what functional roles that individual needs in the MRP AWS GSS and its components.
- All requests for access to the system are verified by user identification and authentication. Users must have a government issued login and password that is controlled and enforced by the USDA eAuthentication application.
- The MRP AWS GSS and its components limit access to relevant information and prevents access to unauthorized information through role-based access.
- All users receive annual security awareness training and are required to sign rules of behavior before being given access to the system. Additionally, all users receive security basics refresher training and sign rules of behavior on an annual basis.

- At the application login screen the warning banner must be acknowledged before users are allowed to log into the application.

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?

The records within the MRP AWS GSS and its components are unscheduled and therefore are considered permanent until the actual records retention scheduled is approved by NARA.

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

The MRP 400 has been submitted for NARA 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.

Unauthorized disclosure of contact information, as identified in Section 1.1 above, is the primary privacy risk, as identified by the PIA. Personally Identifiable Information (PII) is limited to names, addresses, email and phone numbers of submitters/collectors and premises/animal owners. The benefit of having that data available for premises backtracking and other trending information during an emergency overrides any risk due to data retention timescale. All records will be retained as MRP awaits NARA disposition and retention scheduling. MRP AWS GSS and its components maintain information in a secure environment and data is encrypted at rest.

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?

All data is available only (for the areas/states for which they have responsibility) to staff of USDA who has a need to know for the purpose of mission-related activities, program implementation, oversight, and reporting.

4.2 How is the information transmitted or disclosed?

The USDA and state partners have access to VS DIS through the MRP AWS General Support System (GSS) via the Palantir Platform for data entry or viewing or via tools such as Tableau and Alteryx tools for reporting.

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.

Unauthorized disclosure of contact information, as identified in Section 1.1 above, is the primary privacy risk to information shared internally to APHIS. These risks are mitigated through users having direct access to the system. Additionally, the animal health professionals who have access to the data are trained in the proper use and dissemination of this data. All access must be approved, before it is granted. VS, where feasible and within the technical limitations, ensures activities within the VS DIS are audited, PII is used only for authorized purposes and in a manner that is compatible with Privacy Act, and PII use is minimized to the extent necessary to meet the mission needs of the VS surveillance program.

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?

- USDA shares data via the Palantir Platform and VS DIS with cooperating universities and researchers, other Federal agencies (Health and Human Services, Center for Disease Control, and Department of Homeland Security). However, no direct access to the data in the Palantir Platform is provided to these external organizations. USDA staff pulls data as needed. Only summary data will be shared externally. Currently, the only example of routine sharing of PII with external organizations (the public) is limited to Livestock Market Agreements. Here, contact information of Approved Livestock Market owners is made available to the public (first name, last name, phone number, business address) to support identification of USDA VS approved markets for commerce (https://www.aphis.usda.gov/aphis/ourfocus/animalhealth/sa_livestock_markets/ct_approved_livestock_markets).

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.

Where the USDA controls the personally identifiable information in the VS DIS; use of that information will be governed by an appropriate routine use as noted in Section 5.1 above.

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

The MRP AWS GSS and its components currently does not share generally PII data outside USDA. All information sharing is governed by appropriate routine use as noted in Section 5.1 above. Currently, the only example of routine sharing of PII with external organizations (the public) is limited to Livestock Market Agreements. The Livestock Market Agreements data originates from the MiCo tool within the Surveillance Collaboration Service (SCS) system. The data (PII) is transmitted through VS DIS to the USDA EDAPT tool for publishing in a public Tableau dashboard.
https://www.aphis.usda.gov/aphis/ourfocus/animalhealth/sa_livestock_markets/ct_approved_livestock_markets)
Additionally, there are FOIA requests where responses must include PII. For these requests, VS DIS works with agency FOIA contacts to identify the PII and, with their input, the FOIA personnel redact/adjust the records at their discretion. Data is provided by (CFI) to VS personnel working with FOIA (Records Management). VS DIS followa all protocols and standards established by personnel supporting FOIA.

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

The MRP AWS GSS and its components currently does not share data outside USDA. All information sharing will be governed by an appropriate routine use as noted in Section 5.1 above. No PII will be shared externally / outside of USDA.

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.

The MRP AWS GSS and its components are reliant on the SORNs of the source systems. See Section 5.1 for a list of SORNs.

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

N/A: Information is not collected by VS DIS. Therefore, the responsibility of notifying individuals about the collection of their information rests with the owners of the source systems.

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

N/A: Information is not collected by VS DIS. Therefore, all responsibilities regarding the collection of individuals' information rests with the owners of the source systems.

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. The data are treated uniformly. Once the information is submitted to the source systems it is subject to all routine uses as noted in Section 5.1.

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.

The System of Record Notice is the official notice. No information is collected without an individual's awareness. This Privacy Impact Assessment will serve to provide general notice until such time that the SORN is published in the Federal Register. All personally identifiable information is protected and no data will be shared outside the documented Routine Uses without an accounting of the disclosure to the record owner.

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 him or her. Requests for hard copies of records should be in writing, and the request must contain the requesting individual's name, address, name of the system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. 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?

Inaccurate data are corrected by submitting requests to the procedures outlined in the following link: https://www.aphis.usda.gov/aphis/resources/foia/ct_how_to_submit_a_foia_request

Or can be addressed to Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

Procedures are outlined in the SORNs that are identified in Section 5.1.

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

N/A – Redress is provided.

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

An assessment of the privacy risk associated with the redress process is provided by the FOIA/PA staff and director as outlined in Sections 7.2 and 7.4 of this document.

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?

Access to the MRP AWS GSS and its components are based on the need to conduct business with USDA and is approved by an authorized USDA official. Criteria, procedures, and controls are documented. Access must be requested in writing and approved by the supervisor or APHIS authorizing official.

Once access is authorized, users of the Palantir Platform and VS DIS information are further controlled through electronic role-based access. The system is integrated with USDA eAuthentication application and requires level 2 authenticated access. Users must have a government issued login and password that is controlled and managed either at the USDA district or local USDA offices. Password controls, procedures, responsibilities and policies follow USDA departmental standards.

8.2 Will Department contractors have access to the system?

Only specifically authorized USDA contractors have access to the system. Those individuals must first obtain relevant security clearances along with specific authorization to access information at various levels.

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

All USDA employees provided access to the MRP AWS GSS and its components are required to complete annual Information Technology (IT) Security Awareness Training and must sign a Rules of Behavior form prior to receiving access to the information system. System owners and technical staff are required to complete PII training each year.

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

The MRP AWS GSS and its components were granted an Authority to Operate (ATO) on October 9, 2019.

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

The implementation is in accordance with FIP 199/200 Moderate Baseline Security Controls. Access control is a combination of eAuthentication (user credential and authentication) and authorization (VS DIS roles).

The Palantir Platform implements auditing of user actions in the system. User actions are recorded and stored in audit logs accessible only to authorized personnel in USDA.

The audit logs are protected from unauthorized access, modification, and destruction that would negate their value. User auditing captures the following activities: logon and logoff, search query strings, datasets viewed by the user, changes in access permissions, and records/reports extracted from the system. The system also keeps a complete record of all additions, modifications, and deletions of information in the system, the date/time, and user who performed the action.

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?

Unauthorized disclosure of employee and other personnel information, as identified in Section 1.1 above, is the primary privacy risk to information shared both internally and externally to the USDA. This risk is mitigated through technical and procedural information security controls levied on internal and external holders of data.

The Palantir Platform and VS DIS can only be accessed by personnel who have logged in with their e-Authentication PIV or e-authentication username/password credential and have been authorized with specific VS DIS role(s). If data is retrieved, no record of data queried is kept but individual must have user access and rights to access data. Users must be authenticated and have role based access to data which is limited to a need to know basis to the users business unit and teams (Both state level access and commodity group).

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 MRP AWS GSS contains the Palantir Platform and VS DIS as components. VS DIS uses the Palantir platform to integrate animal health data that is culled from operational VS information systems and file uploads. The MRP AWS GSS exists to provide cloud computing services to the MRP Programs. The Veterinary Services program intends to use VS DIS to maximize efficiency, improve business processes, and facilitate comprehensive, integrated surveillance.

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

No

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"?

OMB M-10-23 has been distributed by MRP AWS GSS the system owner and the VS DIS Information Owner.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Not applicable. The MRP AWS 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 MRP AWS 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 MRP AWS 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 MRP AWS 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 MRP AWS 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 MRP AWS 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 MRP AWS 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 MRP AWS GSS does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

Not applicable. The MRP AWS GSS does not use third party websites or applications.

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 MRP AWS 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 MRP AWS GSS does not use third party websites or applications.

Signature authority and protocol differs by agency, we request at a minimum Project Manager/System Owner and ISSPM/CISO sign the document with review by the Privacy Officer.

Agency Responsible Officials

ABHAI SINGH

Digitally signed by ABHAI SINGH
Date: 2022.09.13 09:58:47 -04'00'

Abhai Singh
System Owner
Animal Plant Health Inspection Service
United States Department of Agriculture

Date

Agency Approval Signature

JANELLE JORDAN

Digitally signed by JANELLE JORDAN
Date: 2022.09.13 13:56:40 -04'00'

Tonya Woods
Privacy Act Officer (PAO)
Marketing and Regulatory Programs
United States Department of Agriculture

Date

ANGELA COLE

Digitally signed by ANGELA COLE
Date: 2022.09.13 14:49:00 -04'00'

Angela Cole
Chief Privacy Officer
Deputy Assistant Chief Information Security Officer
Marketing and Regulatory Programs
United States Department of Agriculture

Date