Privacy Impact Assessment
MRP AWS GSS

Policy, E-Government and Fair Information Practices

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

United States Department of Agriculture

Privacy Impact Assessment for the

MRP AWS GSS

August 9, 2019

Contact Point
Elinor Gallelli
USDA APHIS MRP

Reviewing Official
Danna Mingo
MRP Privacy Compliance Officer
APHIS Information Security Branch
United States Department of Agriculture
(301) 851-2487

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)
    - VS NITC System (VNS) 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 Laboratory Information Management System (LIMS)
- This PIA was conducted as part of the initial Assessment and Authorization (A & A).

Overview

The Marketing and Regulatory Programs mission of the USDA is to provide administrative and technical resources to the three agencies – the Agricultural Marketing Service (AMS), Animal and Plant Health Inspection Service (APHIS), and the Grain Inspection, Packers and Stockyards Administration (GIPSA). 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 USDA AWS GovCloud hosting 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 organization 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 upload 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.

Information/Record Type	Component Data (Examples)
Premises	Physical location of a business or animal herd/flock
Premises Supplemental Detail	Commercial operation records to provide additional details about the business, such as type of operation, type, of livestock, and whether or not they are approved to receive international livestock.
Events	Events are activities such as tissue collections, vaccinations, inspections, or inventories.
Surveillance	Test submission information and test results for diseases such as Johnes, Brucellosis, Tuberculosis, Chronic Wasting Disease, Pseudorabies, Swine Influenza Virus, Scrapie or Avian Influenza.
Animal	Animal species, breed, sex, age, classification, and any associated individual or group identifiers.
Other	Specific ad-hoc data, miscellaneous identification numbers such as: the regulatory official ID and/or the Veterinary Accreditation number of the animal health official. It also includes information about the medicine or vaccine name, the manufacturer, and medicine license code.
Status	Temporary conditions or groups that a herd may be part of or subject to, such as quarantined, infected, certified free, or scheduled for future testing.
Aggregated	Instance of surveillance and program data that allows state-wide aggregation of data by species, disease, premises type, herd status and/or location (state, county, zip code).

Concerning the privacy related information there are two types collected in the USDA APHIS VS SCS:

- 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.

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, Vesticular 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 gatekeeper for incoming data routing it or rejecting it as appropriate. Surveillance analysts currently have read only access to the Oracle data for analysis and reporting.

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.

VS LIMS: The following information from VS LIMS 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 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
- Location of Animal
- Total Numbers of Animals
- Herd or Flock size
- Herd or Flock affected
- Herd or Flock Dead
- Date collected
- Collected by
- Authorized by
- Preservation
- Purpose
- Country origin
- Country destination
- FAD Number
- Referral Number
- National Poultry Improvement plan (Y/N)
- Specimen
- Species
- O-Group
- Serotype
- Culture Number
- Clinical Role
- Contract number
- Comments

Slaughtering Establishment Information:

- Establishment ID
- Establishment Name
- Establishment Address
- Establishment City
- Establishment State

- Establishment Zip
- Establishment Country
- Establishment eMail
- Establishment Fax
- Establishment Phone

Tuberculosis Sample Information:

- Food Inspector Name
- Veterinarian Name
- Market Buyer Name
- Market Buyer Address
- Market Buyer City
- Market Buyer State
- Market Buyer Zip
- Market Buyer Country
- Lot number
- Number in Lot
- Number with Lesions
- Slaughter Date
- Dressed Weight
- Live Weight
- Post Mortem Report
- Tissue
- Condition

Diagnostic testing information

- Tests requested
- Disease
- Concentration
- Sex
- Sample ID
- Animal ID
- Age
- Age Unit
- Age Classification

Other

- Tracking information on biological agents and toxins
- Tracking information on reagents.

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 Laboratory Information Management System (VS LIMS) VS Integrated Surveillance Modules (VSISM), 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?

The 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 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. The information is accessed by appropriate VS program staff (statisticians, analysts, epidemiologists, field operations) for program implementation, oversight, and reporting. Summary results and reports of the animal health information are disseminated to collaborators and local, State, Tribal, national, and international partners as needed or required (see sections 4 and 5 for more details about internal and external data sharing).

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.

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.
- 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 and surveillance response activities.

The following data is used from VSLS:

The data is used to support routine animal health surveillance of diseases that are not considered a FAD. To that end, APHIS surveillance programs use it to ensure they have timely and accurate information about animal testing for their respective programs before accepting that data into their various production repositories. Once the data is staged and sent on to the destination VS systems, the use of that information is determined by those systems. VSLS does not function as a repository of record and is used only to support the passing of lab transmissions to the appropriate surveillance systems. The use of information in those systems is governed by those systems, not VSLS.

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 LMS:

Surveillance: Support the ongoing animal health programs that monitor diseases of concern by providing testing results and minimal epidemiological information.

Foreign Animal Disease: Support the ongoing FAD incidents by providing testing results and minimal epidemiological information.

The following data is used from EMRS2:

Data is used by VS to manage and investigate animal disease outbreaks in the United States. The system is used by Federal, State, Tribal, and local animal health officials (and human health officials) for:

- Routine reporting of Foreign Animal Disease (FAD) investigations
- Animal disease surveillance and control programs
- State-specific animal disease outbreaks
- National animal health emergency responses

When other Federal and State emergency response agencies assist USDA with an emergency disease outbreak, they may be allowed limited access to the data in EMRS2. The access will depend upon the MOU in place and the need to know of the other agency. Data will be used for:

- Routine reporting of FAD investigations
- Surveillance and control programs
- State-specific disease outbreaks
- National animal health emergency responses

The following data is used from VSPS:

The data collected from the VSPS source system will be used to support Veterinary Accreditation, Import of Animals, Export of Animals, Interstate Movement of Animals, and Slaughter Horse Transport, all of which are cover under Title 9, Code of Federal Regulations (9 CFR) Animals and Animal Products. The data collected within VSPS will also be used for research, investigative and litigation support, comparative and risk analysis.

The following data is used from ADTIS:

The data collected from the ADTIS source system will be used to support the tracing of animals, the location of animals currently in their possession and the history of locations for those animals and animals that may have been co-mingled with the animal of interest.

The following data is used from VS LIMS:

Records collected from the VS LIMS system support the VS program documentation of the submission forms and the intake of laboratory specimens sent to NVLS for diagnostic testing. Records are used to store information from veterinary diagnostic laboratories, private veterinary practitioners, Federal meat inspectors, Federal field veterinarians, and others for the purpose of returning their test results to them. Each submission is attributed a unique, miscellaneous accession number. For the small number of cases sent to PacBio, the accession number is used to identify only the sample. The accession number does not contain PII and NVSL can use the accession number to link the PacBio results to the original submitter.

Records in the system document the results of individual animal disease testing performed by or under the auspices of the NVSL. Records include official test reports for animal import, export, movement, and program disease status certifications. Also included are official test results for suspected foreign animal disease investigations and for animal diseases targeted by the USDA for control or eradication.

Records in the system provide current and historical data used for detecting animal diseases, conducting emergency responses, conducting and evaluating animal disease control measures, performing epidemiological investigations, and forecasting possible animal disease occurrences and outbreaks.

Animal disease that require more in depth testing is sent to a Pacific Biosciences (PacBio) Single Molecule, Real-Time (SMRT) sequencing platform which is provided by Amazon GovCloud and is used by BNVSL. PacBio is used to meet NVSL' responsibility to characterize and maintain reference strains of diseases of national importance to animal agriculture and public health. Every sample of the 200,000 received annually by NVSL is assigned an accession number that is stored in LIMS. This accession number is included with the shipment and is the only LIMS data associated with PacBio.

The results from PacBio are reviewed, annotated and made publicly available at the National Center for Biotechnology Information (NCBI). The whole genome is then immediately available for any nation managing a disease or outbreak by USDA. The digital output from the PacBio is not stored in LIMS.

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. Other business analysis tools such as Alteryx and Tableau may be used. Statistical modeling and analysis may be performed using 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)?

This is in progress. MRP AWS GSS is taking necessary action to ensure that the MRP 400 is completed and submitted to the MRP IT Information Management Branch for processing to NARA.

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.

Not Applicable – data is not shared with internal organizations.

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 USDA APHIS VS DIS and USDA & MRP AWS GSS security controls as delineated in the current USDA APHIS VS DIS System Security Plan. Further, 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. In the event that privacy act data is shared externally, it is limited to the routine uses in the following SORNs (found at the following site: https://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records):
    - APHIS-2: Veterinary Services – Records of Accredited Veterinarians
    - APHIS-5: National Animal Health Laboratory Network
    - APHIS-8: Veterinary Services – Animal Welfare
    - APHIS-11: Emergency Management Response System (EMRS)
    - APHIS-19: Labware Laboratory Information Management System
    - APHIS-ADTS
- Federal and State animal health officials use the information to monitor the status of an animal disease investigation, document actions taken relating to an animal disease

investigation, track the status of animals susceptible to foreign animal diseases, and assist with managing and analyzing animal disease and surveillance programs.

- Federal and State wildlife agencies use the information to assist in managing and analyzing disease programs and monitoring diseases related to wildlife, feral or alternative livestock.
- Federal or State agencies involved with public health such as the Departments of Homeland Security and Health and Human Services use the information for the purposes of zoonotic disease surveillance or control activities.
- Other appropriate agencies and organizations, whether Federal, State, local, or International, used the information to assist investigating or prosecuting a violation of law or of enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and either arising by general statute or particular program statute, or by rule, regulation, or court order issued pursuant thereto.
- Department of Justice may use the information when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, in litigation, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which the records were collected.
- For use in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee, or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected;
- To appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, a risk of identity theft or fraud, or a risk of harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

- To contractors and other parties engaged to assist in administering the program. Such contractors and other parties will be bound by the nondisclosure provisions of the Privacy Act. This routine use assists the agency in carrying out the program, and thus is compatible with the purpose for which the records are created and maintained;
- To USDA contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends or anomalies indicative of fraud, waste, or abuse; and
- To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

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 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.

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?

The information ingested into the Palantir Platform and VS DIS is not collected from the individual, but pulled from existing source systems. Collection of information about individuals will not be directly entered into Palantir by an individual.

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

Data is not collected directly from individuals. The data is ingested into the Palantir Platform is pulled from 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

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?

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.

An assessment of the privacy risk associated with the redress process is provided by the FOIA 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 is a new system and is following the requirements to receive an Authority to Operate (ATO).

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

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 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.

VS DIS is a browser-based information system that uses the Palantir Platform, which is hosted on a cloud-based platform.

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?

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.

Approval Signature

MARCO MUNOZ
Digitally signed by MARCO MUNOZ
Date: 2019.09.30 10:13:28 -06'00'

Marco Munoz
MRP AWS GSS System Owner
Chief Technology Officer
Animal Plant Health Inspection Service
United States Department of Agriculture

ELINOR GALLELLI
Digitally signed by ELINOR GALLELLI
Date: 2019.09.30 10:06:09 -06'00'

MRP CISO or MRP ISSPM
Animal Plant Health Inspection Service
United States Department of Agriculture

TONYA WOODS
Digitally signed by TONYA WOODS
Date: 2019.09.30 13:18:34 -04'00'

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