USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Data Integration Service (DIS)
Program Office	Veterinary Services
Mission Area	MRP APHIS
CSAM Number	2677
Date Submitted for Review	-

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Angela Cole	202-465-6265
Information System Security Manager	Josh Luterman	970-494-7126
System/Program Managers	Orlando (Rich) Baca	970-494-7346

Abstract

The Data Integration Services system (DIS) is used by the USDA's Veterinary Services (VS) as a tool to integrate and centralize data from multiple VS systems. These VS source systems feed epidemiological information, lab test results, collection site samples and other VS program data into DIS, which allows VS to gain a holistic view of its data and to produce comprehensive reports. This will help VS accomplish its mission by maximizing efficiency, improving business processes, and facilitating comprehensive animal and disease surveillance. The information in DIS includes the personally identifiable information (PII) of members of the public.

Overview

The USDA's Veterinary Services (VS) protects the health and quality of U.S. livestock, animal products and veterinary biologics by monitoring and addressing animal health issues and diseases. VS uses the Data Integration Services (DIS) system to view, analyze, transform, aggregate, and model data across various USDA source systems. These sources. systems integrate directly with DIS to feed data to it (a full list of source systems is included in question 2.2 of this PIA). 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. DIS uses the Palantir Platform, a platform as a service product and replaces the Amazon Web Services General Support System (AWS GSS) previously in use. DIS will also use the Palantir platform for data entry and the uploading of files into data pipelines managed in Palantir. DIS contains the PII of roughly 250,000 individuals. The legal basis for collecting the information in DIS varies depending on the source system (please see question 1 for the full list.)

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

What legal authorities and/or agreements permit the collection of information by the project or system?

- 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

Has Authorization and Accreditation (A&A) been completed for the system?

Yes:

- The Security Plan: Updated and signed on 8/2/2024
- The Authorization Status: Renewed as of 11/18/2024, until 11/18/2027
- The Risk Review Completion Date: 11/18/2024
- The FIPS 199 classification of the system: MODERATE

What System of Records Notice(s) (SORN(s)) apply to the information?

- APHIS 2 Veterinary Services - Records of Accredited Veterinarians
- APHIS 5 National Animal Health Laboratory Network (NAHLN)
- APHIS 8 Veterinary Services - Animal Welfare
- APHIS 11 Emergency Management Response System (EMRS)
- APHIS 15 Animal Health Surveillance and Monitoring System
- APHIS-16 - Animal Disease Traceability Information System (ADTIS)
- APHIS 19 - National Veterinary Services Laboratories' Laboratory Information Management System (NVSL-LIMS)

Is the collection of information covered by the Paperwork Reduction Act?

No.

Section 2: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

What information is collected, used, disseminated, or maintained in the system/program?

Identifying Numbers

- Registration number
- File/Case ID number
- Professional License number
- Name (Including Nicknames)
- Business Mailing Address (sole proprietor)
- Date of Birth (MM/DD/YY)

Biographical Information

- Name (Including Nicknames)
- Business Mailing Address (sole proprietor)
- Date of Birth (MM/DD/YY)
- Business Phone or Fax Number (sole proprietor)
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Personal Email Address
- Business Email Address

What are the sources of the information in the system/program?

This system does not collect any PII directly from members of the public. All PII comes from other APHIS source systems. These consist of:

- Emergency Management Response Services 2.0 (EMRS2)
- Surveillance Collaboration Services (SCS)
    - IdeaGen Mobile Data Collection (MiCo)
    - Mobile Information Management (MIM)
- VS Laboratory Information Management System (VS LIMS)
    - VS Searchable Test Result Application for NVSL Diagnostics (STRAND)
- VS Integrated Surveillance Modules (VSISM)
    - Veterinary Services Analytics Warehouse (VSAW)
- VS Multisystem on Azure Cloud (V-MAC)
    - Animal Disease Traceability Information System (ADTIS)
    - Laboratory Messaging Service (LMS)
        - VS Searchable Test Result Application for NVSL Diagnostics (STRAND)
    - Veterinary Services Laboratory Submissions (VSLS)

    - Veterinary Services Process Streamlining (VSPS)
    - User Fee System (UFS)
- S NCAH on Azure Platform (NAP)
    - User Management System (UMS)
- Veterinary Export Health Certification System (VEHCS)

How is the information collected?

The DIS system primarily collects information directly from the source systems listed in question 2.2 via a direct system integration. In some cases, USDA team members will manually enter information from the source systems into DIS.

Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

No, all PII within DIS comes directly from other USDA systems.

How will the information be checked for accuracy? How often will it be checked?

The DIS system only assists the human evaluation and decision-making processes associated with data retrieved from other systems. Therefore, DIS relies on the system(s) and/or program(s) performing the original collection to provide accurate data. 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 DIS or in the source system, which then pushes the corrected data to DIS. This automated data update process helps to ensure the data in the DIS is as current and accurate as possible.

The Palantir Platform also implements automated data validation rules and checks such as missing data and invalid data entries, which helps reduce data quality issues. Additionally, VS and MRP-IT technical subject matter experts can implement validation rules and data checks programmatically with automated alerts for success or failure as appropriate.

For ad hoc data uploads, in the event uploaded data is later identified as inaccurate, 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 DIS, it is the responsibility of a supervisor or systems administrator to make the appropriate changes to the incorrect data. DIS users are trained in how to modify ad hoc data for accuracy and correctness in the system.

Does the system/program use third-party websites?

No

What is the purpose of the use of third-party websites?

Not Applicable. The DIS system does not use third-party websites or applications.

What PII will be made available to the agency though the use of third-party websites?

Not Applicable. The DIS system does not use third-party websites or applications.

Privacy Impact Analysis: Related to characterization of the information.

Privacy Risk: There is a privacy risk that DIS may have more information that is necessary resulting in the overcollection of data within the system. There is also a risk of inaccurate information, as DIS collects information from multiple different source systems.

Mitigation: All PII within DIS comes from other systems and DIS does not have the ability to limit the scope of collection for other systems. However, DIS only receives the minimum PII from the source systems required to conduct its business functions and reporting. PII in DIS will be maintained only for as long as needed for business purposes once the record retention schedule has been approved by the National Archives and Records Administration (NARA). DIS has several built-in functions that check for missing or invalid data, and DIS users are trained in how to check for and update inaccurate information.

Section 3: Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

The DIS system 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 insight and decision making. DIS allows for a comprehensive view of all the data and creates efficiency across the organizations within one tool that can facilitate improved VS functions, including surveillance response, emergency response, and import/export activities.

Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

DIS combines information from multiple USDA and public sources but does not create new information about individuals or conduct predictive analysis of individuals. Reports are focused on the activities of APHIS.

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk: There is a privacy risk that DIS, and the information it contains, can be used outside of its intended purpose.

Mitigation: The following controls are implemented to ensure that the information is used in accordance with the described and approved uses:

- 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 DIS system 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.
- DIS and its components limit access to relevant information and prevent 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.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

How does the project/program/system provide notice to individuals prior to collection?

This PIA serves as general notice to the public about the types of information that DIS processes and how it's used. The DIS system does not collect any data directly from individuals, and therefore the source systems are responsible for providing notice to the individuals at the time of collection.

What options are available for individuals to consent, decline, or opt out of the project?

The information is not directly collected by DIS. Therefore, the responsibility of consent rests with the source systems at the point of original collection.

Privacy Impact Analysis: Related to notice.

Privacy Risk: There is a risk of individuals will not be aware that their information is processed in DIS.

Mitigation: This PIA is posted publicly and serves as notice of the types of information that are processed in DIS, and how it is used. The information in DIS comes from other source systems and is not collected directly from members of the public. Therefore, providing a Privacy Act Statement or other privacy notice directly to individuals at the time of data collection falls under the purview of those source systems.

Section 5: Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

What information is retained and for how long?

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

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

No. APHIS VS has developed record retention schedules, but until the schedules are submitted and approved by NARA, the electronic systems are classified as permanent in accordance with unscheduled records management policy.

Privacy Impact Analysis: Related to retention of information.

Privacy Risk: The indefinite retention schedule raises the risk of data being compromised, being accessed by unauthorized personnel or becoming inaccurate the longer it is maintained.

Mitigation: The DIS system and its components maintain information in a secure environment in the USDA network and data is encrypted at rest. Access to information is based on roles with a business need to view and update information. Access is requested and granted through the APHIS User Management System. User reviews are conducted quarterly by supervisors to validate user permissions are still accurate. The system also maintains audit logs that record how and when information is updated in case there is suspected unauthorized access.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

DIS receives PII from the internal source systems listed above in 2.2, both via direct system integrations and via manual data entry by USDA team members. Additionally, PII from DIS is transmitted to Tableau (EDAPT) which are used for reporting and the visualization of data.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: The unauthorized disclosure of PII during internal sharing is the primary privacy risk.

Mitigation: All integrations from the source systems to DIS, and from DIS to EDAPT, are secured with encryption to ensure that information is scrambled and unreadable to unauthorized users during transmission. To prevent the unauthorized disclosure of information in cases where USDA team members are manually entering information in DIS, all users receive security basics training and are required to sign rules of behavior before being given access to DIS or any of the systems that share information with DIS. The training and rules of behavior outline the proper sharing of information. DIS users are also provided with roles that limit access to data based on their business need.

With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

The DIS system currently does not share PII outside of the USDA.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: No PII will be shared externally outside of the USDA.

Mitigation: No PII will be shared externally outside of the USDA.

Section 7: Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

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 by submitting a Privacy Act Request or a Freedom of Information Act (FOIA) Request. 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, time frame 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 APHIS Privacy Act Officer, Legislative and Public Affairs, APHIS5601 Sunnyside Ave. Ap-740 Beltsville, MD 20705.

Additionally, each source system listed in #2.2 of this PIA has its own process for individuals to request access to their information. Specific instructions can be found in the individual PIAs for those systems or the SORNs listed in #1.3.

What are the procedures for correcting inaccurate or erroneous information?

Inaccurate data can be corrected by submitting Privacy Act Requests to update information using the procedures listed above in 7.1. Additionally, requests may be made to the source systems as listed above.

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

Procedures on how to submit Privacy Act requests and FOIA requests are posted publicly online and within this PIA. Additionally, each source system posts instructions within their PIAs and within the SORNs listed in #1.3 of this PIA.

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

A formal redress process is provided.

Privacy Impact Analysis: Related to redress.

Privacy Risk: There is a privacy risk that individuals will not be aware of how to access or update their information.

Mitigation: Individuals are provided with the right to submit Privacy Act requests and FOIA requests to access and update their information in the system. Instructions are posted publicly online and within this PIA. Additionally, source systems have their own mechanisms to allow individuals to access and correct their information directly in those systems, as listed in their PIAs and in the SORNs listed in #1.3 of this PIA.

Section 8: Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

How is the information in the system/project/program secured?

The system provides multiple technical safeguards to prevent the misuse of data and APHIS carries out continuous monitoring to ensure that these technical safeguards are in place. These safeguards include:

- Confidentiality: Encryption is implemented to secure data at rest and in transit for the application (HTTPS and database encryption).
- Access Control: Role/feature-based access is used to ensure staff only receive access to limited data for their job responsibilities.
- Authentication: Access to the system is controlled by multi-factor authentication, which requires users to enter a password and an additional means of authentication.
- Session timeout: Users are automatically logged out of the system after a period of inactivity.
- Audit: Logging is implemented for this application, which allows system administrators to view the date and time of the last updates and who made the updates, in cases of misuse of the system or unauthorized access.

What procedures are in place to determine which users may access the program or system/project, and are they documented?

Access to the DIS system and its components is based on business need and is approved by an authorized APHIS official. Access must be requested in writing and approved by the supervisor or APHIS authorizing official.

Once access is authorized, the use of DIS information is further controlled through electronic role-based access, which ensures that users have limited access to information that they need for their job responsibilities. Multi-factor authentication is used, which ensures that users are required to provide a password and an additional form of authentication. Password controls, procedures, responsibilities, and policies follow USDA departmental standards and are part of a documented process.

How does the program review and approve information sharing requirements?

The DIS system currently does not share PII data outside of the USDA. All new information sharing requests would be reviewed by the system owner and system Information System Security Officer (ISSO).

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

Prior to receiving access to DIS, all USDA employees are required to complete annual Information Security Awareness Training.