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	

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Surveillance Collaboration Services (SCS)
Program Office	Veterinary Services
Mission Area	MRP
CSAM Number	1931
Date Submitted for Review	**TBD**

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Angela Cole	angela.cole@usda.gov	202-465-6265
Information System Security Manager	Josh Luterman	Joshua.Luterman@usda.gov	970-494-7126
System/Program Managers	Orlando (Rich) Baca	orlando.r.baca@usda.gov	970-494-7346

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

The USDA Animal and Plant Health Inspection Service (APHIS) Veterinary Services (VS) Surveillance Collaboration Services (SCS) supports routine animal health surveillance and program management under the purview of VS Surveillance, Preparedness and Response Services (SPRS). It provides comprehensive, coordinated, and integrated animal health surveillance and program management software that serves as the foundation for animal health, public health, food safety, and environmental health. SCS supports the function of managing data related to animal health surveillance and response to animal health events, including data storage, analysis and reporting. SCS collects the PII of the owners of premises and animals that are the subject of animal disease events and the PII of state animal health officials who work with the USDA on animal disease surveillance and mitigation efforts.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

VS SCS is a collection of multiple commercial off-the-shelf software (COTS) platforms and USDA developed services focused on animal health and surveillance. VS SCS enables VS to perform comprehensive surveillance of animal health for numerous species and diseases to facilitate the detection, management, prevention, investigation, control and eradication of animal diseases.

VS SCS maintains test and/or vaccination data and other program information such as disease or certification status for flocks/herds subject to or involved with APHIS VS animal disease/pest surveillance and/or control programs. Included in this functional data is privacy related data such as USDA and State employee name, address, phone number and email address for employees directly involved in the above-mentioned program activities. VS SCS also maintains name, address, phone number and email address for individuals identified as contacts for premises (locations) and owners of animals or animal-related operations involved with the various programs. Because of the variable 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. VS SCS supports the VS mission to protect and improve the health, quality, and marketability of our nation's animals by providing a nationwide repository of animal health and productivity information.

Data from all SCS components are aggregated in VS Data Integration Services (DIS) and the USDA Enterprise Data Analytics Platform & Toolset (EDAPT) for data processing, analysis and visualization purposes. The information in SCS is authorized to be collected under the Animal Damage Control Act of 1931, the Animal Health Protection Act, the Farm Security and Rural Investment Act of 2002, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, the Homeland Security Presidential Directives 7 and 9, and the Farm Bills.

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.

1.1. 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. 8351 et seq. of the Animal Health Protection Act
- The Animal Health Protection Act, 7 U. S. C. 8301-8317
- The Farm Security and Rural Investment Act of 2002, 7 U.S.C. 7901 et seq.
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002, 116 Stat 674-678
- The Homeland Security Presidential Directives 7 and 9; and
- Farm Bills - an omnibus, multiyear law that governs an array of agricultural and food programs

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

Yes:

- The Security Plan: Updated and signed on 9/08/2023
- The Authorization Status: Renewed as of 9/11/2023 until 9/11/2026
- The Risk Review Completion Date: 9/11/2023
- The FIPS 199 classification of the system: MODERATE

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

APHIS-15 covers the collection of information in the system.

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

Yes. OMB forms are not required for input into Surveillance Collaboration Services, but forms used for data entry are: VS 1-27 (OMB #s 0579-0047, 0065, 0101, 0127, 0146, 0338, 0393, 0453), VS 4-33 (OMB # 0579-0047), VS 4-54 (OMB #0579-0047), VS 5-19a and b (OMB #s 579-0015, 0049, 0054, 0088, 0124, 0155, 0187, 0310, 0322, 0337, 0346, 0363 0383, 0450), VS 6-22 (OMB #s 0579-0146) and VS 10-4 (OMB #s 0579-0040, 579-0090, 0579-0101, 0579-0146, 0579-0189, 0579-0485).

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.

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

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers

☐ Social Security number	☐ Truncated or Partial Social Security number	☐ Driver's License number
☐ Passport number	☐ License Plate number	☐ Registration number
☐ File/Case ID number	☐ Student ID number	☐ Federal Student Aid number
☐ Employee Identification number	☐ Alien Registration number	☐ DOD ID number
☐ Professional License number	☐ Taxpayer Identification number	☐ Business Taxpayer Identification number (sole proprietor)
☐ Credit/Debit Card number	☐ Business Credit Card number (sole proprietor)	☐ Vehicle Identification number
☐ Business Vehicle Identification number (sole proprietor)	☐ Personal Bank Account number	☐ Business Bank Account number (sole proprietor)
☐ Personal Device Identifiers or Serial numbers	☐ Business Device Identifiers or Serial numbers (sole proprietor)	☐ Personal Mobile number

☐ Health Plan Beneficiary number
☐ Business Mobile number (sole proprietor)
☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)
☒ Business Mailing Address (sole proprietor)
☐ Date of Birth (MM/DD/YY)

☐ Ethnicity
☒ Business Phone or Fax Number (sole proprietor)
☐ Country of Birth

☐ City or County of Birth
☐ Group Organization/Membership
☐ Religion/Religious Preference

☐ Citizenship
☐ Immigration Status
☒ Home Phone or Fax Number

☒ Home Address
☐ ZIP Code
☐ Marital Status

☐ Spouse Information
☐ Children Information
☐ Military Service Information

☐ Race
☐ Nationality
☐ Mother's Maiden Name

☒ Personal Email Address
☒ Business Email Address
☐ Global Positioning System (GPS)/Location Data

☐ Employment Information
☐ Alias (Username/Screenname)
☐ Personal Financial Information (Including loan information)

☐ Education Information
☐ Resume or Curriculum Vitae
☐ Business Financial Information (Including loan information)

☐ Professional/Personal References

Biometrics

☐ Fingerprints
☐ Hair Color
☐ DNA Sample or Profile

☐ Retina/Iris Scans
☐ Video Recording

Distinguishing Features

☐ Palm Prints	☐ Eye Color	☐ Signatures
☐ Dental Profile	☐ Photos	

Characteristics

☐ Vascular Scans	☐ Height	☐ Weight
☐ Scars, Marks, Tattoos	☐ Voice/Audio Recording	

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)	☐ Cell Tower Records (e.g., Logs, User Location, Time)	☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information	☐ Mental Health Information	☐ Disability Information
☐ Workers' Compensation Information	☐ Patient ID Number	☐ Emergency Contact Information

Specific Information/File Types

☐ Personnel Files	☐ Law Enforcement Information	☐ Credit History Information
☐ Health Information	☐ Academic/Professional Background Information	☐ Civil/Criminal History Information/Police Record
☐ Case Files	☐ Security Clearance/Background Check	☐ Taxpayer Information/Tax Return Information

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

The premises and animal owners subject to animal disease surveillance/activities provide their own PII. In some cases, they provide their PII to state animal health officials who then enter the information into SCS.

State employees working on animal disease surveillance activities provide their own PII.

2.2.1. How is the information collected?

The owners of premises or animals submit their PII on the OMB-approved forms listed in question 1.4 and email or physically mail them to the USDA or state animal health official who then enters the information in the system. In some cases, the premises or animal owners will provide this information over the phone to the USDA or state animal health official who then enters the information into the system.

State workers submit their information via the USDA User Management System in order to be furnished with an account in SCS and assigned a role in the system.

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

No

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

Data collected from both customers and USDA sources is verified for accuracy, relevance, timeliness and completeness by USDA and state employees who are trained in entering accurate data as part of their operational duties. These employees are responsible for the review and accuracy of the data. Verification of data records occurs at the time data is collected and on an as-needed basis. Also, there are limited systematic data entry constraints, such as the use of data validation fields, to ensure entry completeness and to help reduce data from being entered into the incorrect field.

2.5. Does the system/program use third-party websites?

No

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

N/A

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

N/A

2.6. **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: The collection of unneeded or extraneous PII, as well as information associated with or linked to individuals creates privacy risks. Additionally, inaccurate information about individuals poses risks related to the characterization and use of personal records.

Mitigation: Personal information and associated data are only collected and used for the intended purposes of the system as outlined in the SORN. The collection minimizes only information required for the system's mission of testing and monitoring animal health. All personal information, whether direct identifiers or information associated with individuals, is collected directly from the data subjects and verified for accuracy.

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.

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

The data in the Surveillance Collaboration Services system is being collected to facilitate the detection, management, prevention, investigation, control and eradication of animal diseases.

The names, addresses, phone numbers and email addresses of the premises and animal owners collected in the Surveillance Collaboration Services system allow animal health officials to effectively communicate with them about animal disease events affecting their animals or properties.

The names, addresses, phone numbers and email addresses of state animal health officials are used to understand who is working on animal disease activities and to be able to communicate and coordinate with them about their work. It is also used to furnish the state workers with SCS accounts and assign them roles within the system.

3.2. 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.

No

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy Risk: There is a risk of PII being used outside of the intended purposes.

Mitigation: SCS adheres to the APHIS-15 SORN which lays out the PII being collected as well as how it is used. Information in SCS is not used for any other purposes. Access to the system is managed via the USDA User Management System and requires USDA supervisor and system owner approval. To access any system, users must pass the Information Security Awareness Training (ISAT) which details the proper handling of PII.

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.

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

The APHIS 15 SORN and this PIA serve as public notice to individuals about the types of information collected in VSISM, the purpose of the collection, and how the information is used.

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

Individuals must provide certain information in order to receive animal health services from APHIS. There is no federal law requiring individuals to provide information, unless they are requesting a service or product from APHIS; however, individuals involved in animal disease investigations may be required to provide information as governed by specific animal health laws and regulations of the state in which they reside.

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: There is a risk of the lack of transparency with individuals regarding the collection and use of their information if a Privacy Act Statement is not provided at the time of collection

Mitigation: SCS adheres to the APHIS-15 SORN which lays out the PII being collected as well as how it is used and is posted publicly online. This PIA also serves as notice. A Privacy Act Statement is currently being developed as well and will be added to forms that are used to collect information for SCS.

.

Section 5: Data Retention

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

5.1. What information is retained and for how long?

Currently, all SCS records will be permanently maintained until a NARA disposition schedule has been approved.

SCS maintains information, including older information that is waiting NARA approval for deletion, in a secure manner, as outlined in question #8.1 of this PIA.

5.2. 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.

Yes, records schedule number: DAA-0463-2017-0002.

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: There are risks related to the long-term retention of unneeded or outdated information, both from a minimization and security standpoint, the longer information is retained, the less likely it is needed and the more likely it is to be compromised.

Mitigation: SCS only collects the minimum amount of information needed to carry out the intended business purpose.

Section 6: Information Sharing

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

6.1. 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?

The personal information in SCS (names, addresses, phone numbers and email addresses of the premises and animal owners) is shared with the USDA Office of the Chief Information Officer's Data Lake environment (EDAPT). EDAPT allows for the visual reporting of data using Tableau and allows USDA team members to review the data and be able to understand the locations of animal disease events to help with mitigation efforts. It is also used to contact the owners of premises about activities on their properties and the owners of animals about their animal health statuses and animal test results. The transmission of the data occurs on an automated schedule over approved and secured internal networking channels between the systems.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: The unauthorized disclosure of contact information during the internal transmission of information, as identified in the section above, is the primary privacy risk.

Mitigation: The integration with EDAPT is secured by the USDA network. All users receive security basics training and are required to sign rules of behavior before being given access to any of the systems that receive information from SCS.

6.3. 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?

Information within the SCS system is generally not shared externally outside of the USDA, beyond the State and local government users who are helping the USDA in disease surveillance and mitigation efforts. These individuals access the same information as USDA employees through direct access to the system. Additionally, there may be exceptional cases of external sharing, such as in a data breach or legal case, and these are outlined in the routine uses section of the SORN.

6.4. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: There is a risk of inappropriate use, retention, or further disclosure of personal information by authorized external users, or failure to maintain appropriate safeguards for information accessed through their legitimate system access.

There is the risk of unauthorized access to information for external state animal health officials.

Mitigation: All external users must request access through the USDA User Management System (UMS), and demonstrate a business need to access the system. A USDA supervisor must review the request and approve it before a system owner provides access. Roles are assigned in the system to state animal health officials that limit their access to information to only what they need for their official duties. For example, a state animal health official can only view information related to their state. All users are trained in information security before accessing the system, including the importance of maintaining the confidentiality of information.

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.

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 by submitting a Privacy Act Request or Freedom of Information Act (FOIA) request. Requests may be submitted using the APHIS Privacy Act/FOIA Portal, via Phone: 301-851-4102, Fax: 301-734 –5941 or email: foia.officer@aphis.usda.gov. Requests may also be sent via mail. Requests for hard copies of records should be in writing, and the request must contain the requesting individual's name, address, name of 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 APHIS Privacy Act Officer, Legislative and Public Affairs, APHIS5601 Sunnyside Ave. Ap-740 Beltsville, MD 20705.

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

If data is found to be inaccurate, the requestor is directed by the APHIS Privacy Act Officer to formally request correction by using the contact information listed above in question 7.1. Customers can also contact the APHIS or state office where they first provided the information and request correction of inaccurate or erroneous information.

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

Individuals are notified via this PIA as well as the System of Record Notice (SORN). Additionally, APHIS posts the instructions on how to submit FOIA and Privacy Act requests publicly on its website.

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

N/A, there is a formal redress process.

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

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

Mitigation: Individuals are notified of the procedures to correct their information in the SORN and this PIA. Additionally, APHIS publicly posts instructions on how to submit FOIA and Privacy Act requests on its website, as listed above.

Section 8: Auditing and Accountability

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

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

Auditing measures are applied in accordance with FIPS 199/200 Moderate Baseline Security Controls. Some of the technical safeguards for SCS use the Dynamics CRM security model that includes auditing, role-based views, field-level security, and division of security. This means any event, such as creating, modify, delete, old, and new values are audited at the field level to understand who made a change to a record and when they made it. Even the audit history on individual record and audit history summary is tightly controlled with separate security settings to protect the integrity of the log. The security model provides users with access only to the appropriate levels of information based on their role(s). Furthermore, views and field-level are role-based as well, preventing users from seeing, accessing, and/or making changes to individual fields or records to which they do not require access for their job function. Finally, access control is a combination of eAuthentication (user credential and authentication) and authorization (SCS roles).

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

Access to SCS is based on the need to conduct business with USDA and is approved by an authorized APHIS VS official. Criteria, procedures, and controls are documented. Access for federal employees or state workers must be requested via the USDA User Management System (UMS) and approved by the supervisor or APHIS authorizing official. The application owner then reviews the request, and if approved, provides access to the system.

Once access is authorized, users of SCS information are further controlled through electronic role-based access, which ensures that access to information is limited to what a user needs to carry out their work. For example, state animal health officials can only view information relevant to their state. The system is integrated with the 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 Veterinary Services district or local VS offices. Password controls, procedures, responsibilities and policies follow USDA departmental standards.

8.3. How does the program review and approve information sharing requirements?

For any new information sharing requests, discussions are held between the System Owner and Information System Security Officer to determine the requirements. Once the information sharing has been properly reviewed and approved, depending on which is needed, either an Interconnection Security Agreement (ISA) or a Memorandum of Understanding (MOU) will be developed and signed by all required parties.

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

All users receive the USDA Information Security Awareness Training and are required to sign rules of behavior before being given access to the system. Additionally, all users review the training and sign rules of behavior on an annual basis.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 9/24/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

Signed: TRACY HENDRIX Digitally signed by TRACY HENDRIX Date: 2025.09.24 21:18:58 -04'00'

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed: ORLANDO BACA Digitally signed by ORLANDO BACA Date: 2025.09.25 06:55:28 -06'00'

Sunny Geiser-Novotny
System Owner
Marketing and Regulatory Programs
U.S. Department of Agriculture

Signed: ANGELA COLE Digitally signed by ANGELA COLE Date: 2025.09.30 11:26:10 -04'00'

Angele Cole
Acting Assistant Chief Information Security Officer / Mission Area Privacy Officer
Marketing and Regulatory Programs
U.S. Department of Agriculture