Privacy Impact Assessment
Surveillance Collaboration Services (SCS)

Technology, Planning, Architecture, & E-Government

- Version: 2.3
- Date: June 2, 2023
- Prepared for: Marketing and Regulatory Programs

United States Department of Agriculture

Privacy Impact Assessment for the

Surveillance Collaboration Services (SCS)

June 2023

Contact Point
Neil Wyman
USDA APHIS Veterinary Services

Reviewing Official
Tonya Woods
Director, Freedom of Information and Privacy Act Staff
United States Department of Agriculture
(301) 851-4076

Abstract

- This Privacy Impact Assessment (PIA) is for the USDA, Animal and Plant Health Inspection Service (APHIS), Veterinary Services (VS), Surveillance Collaboration Services (SCS) components: SCS CoreOne Web, SCS Mobile Information Management (MIM), Animal Health Services (AHS) and SCS Mobile Forms.
- VS SCS is a collection of multiple commercial off the shelf (COTS) platforms and USDA developed services. VS SCS allows for the collection and reporting of animal health and surveillance information. It provides an electronic means of data input, data transmission, data storage, and data reporting. This enables USDA APHIS to take a comprehensive and integrated approach to collecting and managing animal health data for disease management and surveillance programs.
- This PIA was conducted as part of the annual assessment documents update.

Overview

VS SCS is a collection of multiple 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, and phone information for employees directly involved in the above-mentioned program activities. 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.

VS SCS also 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 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.

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?

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

- Employee information – 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 information – 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, permits, etc.) 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 entitled to protection under the Privacy Act.

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

There are three sources of information for VS SCS: Federal, State/Tribal/Local Government and third-party. Information in this system comes primarily from the users and individuals and/or businesses in the general public involved in or supporting the production, management or holding of livestock. In addition, the USDA Food Safety Inspection Service (FSIS), Farm Services Agency (FSA), and APHIS (Veterinary Services and Wildlife Services), will provide data to the system.

The individual State Veterinarian Offices, as well as multiple state and university animal diagnostics and genotyping testing laboratories will provide data for use in the USDA APHIS VS SCS system.

Third party sources of information may include the American Veterinary Medical Association (AVMA), National Turkey Federation (NTF), and private genotype testing laboratories, private individuals and companies who are the subject of the programs for whom we keep data and third-party data suppliers.

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

The purpose of the Surveillance Collaboration Services system is to allow animal health officials to effectively manage animal disease, pest and surveillance programs including providing:

a) rapid detection and effective response to animal disease and animal pest events in the United States thereby reducing the spread of infections to new flocks/herds;

b) epidemiological analysis, including animal tracing, diagnostic testing, surveillance activities, and other factors of epidemiologic importance for evaluating disease risk;

c) notification to owners or buyers of potentially exposed or infected livestock and State and Federal regulatory officials, including notification through a public web site when records are inadequate to trace such animals to a specific owner or premises;

d) documentation of U.S. animal health program expenditures, statistical data and accomplishments that support national animal disease control programs and international trade agreements;

e) documentation of compliance with and provisions for a public listing of participants in voluntary certification or quality assurance programs; and

f) provide a public listing of approved or qualifying facilities such as approved livestock markets.

1.4 How is the information collected?

The information collected from states, users, individuals and/or businesses in the general public is collected on OMB approved- forms or directly as referenced in As these packages come up for renewal appropriate screen shots will be included. In some cases, the information is entered directly into the USDA APHIS VS SCS CoreOne Web application by animal lab employees who are entering results from their internal lab documents or a state or federal employee entering information provided over the phone, in an email, or letter by a producer to fulfill a request for a flock ID or ear tags. State or federal employees and private practitioners can also enter field data directly into the SCS AHS component. Members of the public do not have access to to enter data themselves.

How will the information be checked for accuracy?

Data collected from both customers and USDA sources is verified for accuracy, relevance, timeliness and completeness by USDA and state employees. These employees are responsible for the review and accuracy of the data. Verification of data records occurs on an as-needed basis. Also, there are limited systematic data entry constraints to ensure entry completeness.

Data collected from non-USDA sources will be verified for accuracy, relevance, timeliness and completeness by USDA Veterinary Services employees, state employees and or other federal employees. These employees are responsible for the review and accuracy of the data. Data verification occurs on an as-needed basis. Also, there are limited systematic data entry constraints to ensure entry completeness.

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

- 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.

1.7 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. USDA APHIS, including the VS Executive Team, District and Commodity Directors, Assistant District Directors, Centers for Epidemiology and Animal Health (CEAH), Center for Informatics (CFI) and State Veterinarians are all responsible for protecting the privacy rights of the employees and other persons identified in the SCS as required by applicable State and Federal laws. Specific mitigation activities are:

- Information that is disclosed must have the signatory approval of the Information System Owner, the Assistant Chief Information Security Officer (ACISO), and VS Authorizing Official. This mitigates the risk of unauthorized disclosure by ensuring no data is release without presentation of these signatures on the applicable signed document.
- Least privilege is implemented to ensure users only have access to the relevant data for their own state. The primary implementation is through assignment of roles to user accounts. Each role is mapped to a collection of permissions to access system data and functionality. Administrative roles have the broadest access to system data. All users are restricted to the information only pertaining to their particular office while others may have access to multiple sets of data. This serves to mitigate the risk of unauthorized disclosure.
- Data is audited at a row level and captured in history tables (data, time and action taken). Audit data is protected from modification and is correlated at an Enterprise level. This mitigates the risk of unauthorized disclosure as a preventative measure.
- All organizational users are required to complete USDA mandatory information security awareness training on an annual basis, which mitigates through user education on what privacy information is and how to properly protect it. It also outlines responsibility and accountability for collecting accurate information and ensuring such information is not disclosed without approval.

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 premises and personal data is used for routine animal health surveillance, management of domestic animal disease and pest control programs, and to monitor for and respond to the introduction of foreign animal diseases to coordinate any outbreak response, deployments, and animal/premises owner notifications.

State Veterinarians and State/Tribal Animal Health officials, as co-owners of the data, have the discretion to share information stored in the VS SCS relevant to premises or persons within their state in accordance with state laws and regulations via public web sites and/or may store such information in animal health and surveillance management databases developed by State IT developers, contractors or other third-party software vendors in a manner that provides secure data access.

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

VS SCS platforms / services use multiple tools to analyze data such as IBM® Enterprise Cognos®, Excel spreadsheets, SAS® (a statistical application), Tableau®, Palantir® Data Integration Services (DIS). Data is used to produce summary reports for stakeholders, and detailed internal reports, which may contain name, address, and phone information for persons identified in VS SCS.

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

VS SCS uses Google Mapping data and USDA National Agriculture Statistics Service (NASS) animal and farm population Census data aggregated at the county level for spatial display. This data allows APHIS to see how much surveillance has been completed by Veterinary Services versus how many animals are reported to live in a particular county.

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.

- VS SCS has 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 VS SCS.
- 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 managed either at the Veterinary Services, National, District or local offices or in the case of local State databases the State Veterinarian's office. Multifactor authentication is enforced for organizational users

- VS SCS limits access to relevant information and prevents access to unauthorized information through role-based access. VS approves access through the User Management System (UMS) and performs quarterly recertifications.
- Detailed reports that include personally identifiable information will be marked as including such data.
- All users take mandatory Information Security Awareness Training (ISAT) and are required to sign the accompanying Rules of Behavior (ROB) before being given access to the system. Additionally, all users must complete ISAT and sign a new ROB annually to retain their access. This training provides mitigation through deterrence of policy violation as well as continuous education.

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 USDA APHIS SCS applications are considered permanent until the actual records retention schedule 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)?

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

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 employee and customer personal data, as identified in Section 1.1 above, is the primary privacy risk, as identified by the PTA. Personally Identifiable Information (PII) is limited to names, addresses, email and phone numbers of submitters. 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. However, all records are retained permanently as VS awaits NARA disposition and retention scheduling. To mitigate this risk, authorization for access is strictly enforced and monitored. Sharing of information with partner agencies, external to USDA, requires that an Interconnection Security Agreement be completed, reviewed and approved by executive leadership of both IT systems, including the Authorizing Official. VS SCS

maintains information in a secure manner and disposes of information per APHIS Directive 3440.2.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Data is not shared with any internal organizations.

4.2 How is the information transmitted or disclosed?

N/A.

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.

N/A.

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?

- To State/Tribal animal health officials and their contractors and other cooperators authorized access by State/Tribal animal health officials, data from their State/Tribe as co-owners of the data to: (a) Collaborate with USDA in conducting, managing, and evaluating animal health, disease, or pest surveillance or control programs, and monitoring for animal health, diseases or pests; (b) aid in containing and responding to a foreign or domestic animal disease or pest outbreak, bioterrorism, or other animal health emergency; (c) disseminate information and solicit feedback on emergency preparedness and response guidelines and the system itself for the purpose of educating and involving these officials in program development, program requirements, and standards of conduct; and (d) States/Tribes may share information on premises, persons, or animals within their State or Tribe in accordance with State or Tribal laws and regulations via public websites or other means;
- To Federal, State/Tribal, or local wildlife agencies to collaborate with USDA in conducting, managing, or evaluating animal health, disease or pest surveillance or

control programs, and monitoring for animal health issues, diseases, or pests affecting both wildlife and domestic animals or respond to emergencies impacting wildlife and domestic animals. Such parties will be bound by the nondisclosure provisions of the Privacy Act;

- To Federal, State/Tribal, or local government agencies involved with public health such as the Departments of Health and Human Services and Homeland Security (DHS) for the purposes of collaborating with USDA to conduct, manage, or evaluate zoonotic disease or pest awareness, surveillance, response or reporting activities, or to respond to emergencies impacting humans and domestic animals;
- To DHS' Customs and Border Protection for inspection of compliance with permit conditions;
- To cooperating laboratories, Federal, State, and local government officials, employees, or contractors, and other parties engaged to assist in administering animal health programs to assist the agency in carrying out the program. Such contractors and other parties will be bound by the nondisclosure provisions of the Privacy Act;
- To the World Organization for Animal Health (Office International des Epizooties (OIE)) for reporting summarized animal diseases information and to document country or regional disease status. No customer, employee, or other classification of private information is published or distributed to the OIE;
- To USDA contractors or cooperators with signed agreements collaborating with USDA in conducting, managing, or evaluating animal health, disease or pest surveillance or control programs, and monitoring for animal health issues, diseases, or pests or to aid in containing and responding to a foreign or domestic animal disease outbreak, zoonotic disease outbreak, bioterrorism, radiological event, or other animal health emergency;
- To the public through USDA websites: (a) Lists of participants in voluntary animal disease certification or quality assurance programs; (b) lists of individuals or entities not in compliance with animal disease regulations to reduce the potential risk of animal disease spread; and (c) list the herds of origin of exposed or potentially exposed animals when needed to notify individuals who may have acquired exposed or potentially exposed animals when other means of contact are unavailable.
- To the public and trading partners for their information and dissemination as needed and to document country or regional disease status. These summarized reports do not contain any customer, employee or other classifications of private data;
- To appropriate law enforcement agencies, entities, and persons, whether Federal, foreign, State, Tribal, local, or other public authority responsible for enforcing, investigating, or prosecuting an alleged violation or a violation of law or charged with enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, when a record in this system on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or court order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutive responsibility of the receiving entity;
- To the Department of Justice when: (a) USDA, or any component thereof; or (b) any employee of USDA in his or her official capacity where the Department of Justice has

agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, USDA determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by USDA to be for a purpose for which USDA collected the records;

- To a court or adjudicative body in a proceeding when: (a) USDA or any component thereof; or (b) any employee of USDA in his or her official capacity; or (c) any employee of USDA in his or her individual capacity where USDA has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, USDA determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by USDA to be for a purpose that is compatible with the purpose for which USDA collected the records;
- To appropriate agencies, entities, and persons when: (a) USDA suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) USDA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, USDA (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;
- To another Federal agency or Federal entity, when information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the agency (including its information systems, programs, and operations), the Federal Government, or national security;
- To a Congressional office in response to an inquiry made at the written request of the individual to whom the record pertains;
- To USDA contractors and other parties engaged to assist in administering the program, analyze data, information management systems, Freedom of Information Act requests, and audits. Such contractors and other parties will be bound by the nondisclosure provisions of the Privacy Act;
- 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 (NARA) or to other Federal government agencies pursuant to records management activities being conducted under the authority of 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.

Yes. Where the USDA controls the personally identifiable information in the SCS; use of that information will be governed by an appropriate routine use in Animal Health, Disease, and Pest Surveillance and Management System, USDA/APHIS-15. APHIS VS works with State authorities on data protection through the use of Non-Disclosure Agreements (NDAs), Interconnection Security Agreements (ISAs), Memorandum of Understandings (MOUs) and other agreements.

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

Information shared outside the Department falls within the disclosures outlined in section 5.1. The data is extracted per the requested parameters and is then transmitted to the requesting internal point of contact using secure protocols and connections.

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

The risk identified as a result of external sharing is the potential release of inaccurate data. The risk to inaccurate data is mitigated at the point of collection when the information owner is asked to verify the data inputted by the employee is accurate before it is saved in the SCS. Safeguards, such as, security and privacy training for organizational personnel is required, so employees are able to identify PII data and safeguard it in approved ways. Governance and technical procedures restrict data access to only those allowed by the user. Finally, all requests for the sharing of PII, whether the request comes as a result of a routine use or not, must be reviewed/approved by the VS Executive Leadership, the System Owner, the VS Authorizing Officer and the APHIS Cyber Security Services Branch.

Section 6.0 Notice

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

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

Yes. The APHIS 15 SORN is the official notice. **Regulations.gov.**

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

Individuals must provide certain information in order to receive animal health services from the APHIS. There is no law requiring individuals to provide information, unless they are requesting a service or product from APHIS. Further, individuals involved in animal disease investigations are required to provide information as governed by specific animal

health laws and regulations of the state in which they reside. Efforts are currently underway to add a Privacy Act notice to all electronic forms/pages within the system.

6.3 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 for all submitters. Once the information is submitted it is subject to all routine uses.

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

The System of Record Notice is the official notice.

Information is collected in the field using various VS Forms. Currently the forms do not provide the required notice to individuals regarding collection of information. There is an effort underway to update the forms to properly inform all parties at the point of information collection.

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?

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the APHIS Privacy Act Officer, 4700 River Road Unit 50, Riverdale, MD 20737 or by email: APHISPrivacy@usda.gov. If an individual believes more than one USDA component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Act Officer, Department of Agriculture, 1400 Independence Avenue, SW, Washington, DC 20250.

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

Members of the public are advised to submit requests to correct inaccurate or erroneous to the APHIS Privacy Office, as indicated above.

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

Individuals are notified of procedures by the APHIS 15 SORN and by animal health officials at the point of data collection.

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

If an individual believes that they suffered an adverse consequence related to inaccuracies within the system, that individual will be able to provide any information that they deem relevant with a request that it be included within any record maintained in the system regarding a particular incident, activity, transaction, or occurrence.

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 VS 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 must be requested in writing and approved by the supervisor or APHIS authorizing official.

Once access is authorized, users of VS SCS 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 Veterinary Services district or local VS offices or in the case of local State databases the State Veterinarian's office. Password controls, procedures, responsibilities and policies follow USDA departmental standards.

.

8.2 Will Department contractors have access to the system?

Yes.

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

All APHIS employees provided access to VS SCS are required to complete annual USDA Information Security Awareness Training and must sign accompanying Rules of Behavior prior to receiving access to the information system. VS 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?

Yes. VS SCS renewed its Authority to Operate (ATO) on September 30, 2020 by completing an Assessment and Authorization. The ATO for this system will be renewed on or before September 30, 2023.

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

Formal auditing measures for VS SCS will include security assessments performed by USDA APHIS at least annually and independent security assessments performed in support of Assessment and Authorization efforts. The independent assessments will be performed per the timeframe of VS SCS Authority to Operate schedule.

As to technical safeguards:

- The VS SCS is continuously monitored in several different ways. MRP Azure Cloud systems are scanned every thirty days to identify possible threats. The vulnerabilities identified are required to be remediated by the responsible parties.
- Access control technical measures are in place and operating to ensure only users with approval can access the data, and the concept of least privileged is enforced to ensure only the minimum access and privileges are granted to enable users to perform the job function. User access is audited on a continual basis.
- Operational technical safeguards to prevent data misuse begin with access control. SCS employs TLS encryption to protect data during transmission and enforces multifactor authentication for user access. Password controls, procedures, responsibilities, and policies follow USDA departmental standards. APHIS employees must use LincPass to access their computer and the APHIS network, including the VPN. There is no action that can be performed within the SCS without identification and authentication.
- At the USDA and APHIS Enterprise level, intrusion detection and intrusion prevention, firewalls and antivirus measures are employed on a continuous basis.

8.6 <u>Privacy Impact Analysis</u>: 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?

The privacy risk associated with access and security controls is the unauthorized or inappropriate access of data in the system. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy.

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 VS SCS is a major application (MA) that collects, manages, and evaluates animal health data for disease management and surveillance programs.

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

VS SCS does not employ technology which may raise privacy concerns.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

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

Not applicable. VS SCS 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. VS SCS 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. VS SCS 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. VS SCS 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. VS SCS 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. VS SCS 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. VS SCS 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. VS SCS does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

Not applicable. VS SCS 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?

No, not applicable.

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. VS SCS does not use third party websites or applications.

Responsible Officials

_____
Neil Wyman
System Owner
United States Department of Agriculture

Approval Signature

_____
Tonya Woods
APHIS Privacy Act Officer
United States Department of Agriculture

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