Privacy Impact Assessment

Veterinary Services Integrated Surveillance Modules (VSISM)

Policy, E-Government and Fair Information Practices

- Version: 1.5
- Date: April 18, 2023
- Prepared for: USDA Marketing and Regulatory Programs

United States Department of Agriculture

Privacy Impact Assessment for the

Veterinary Services Integrated Surveillance Modules (VSISM)

April 2023

Contact Point
Neil Wyman
USDA APHIS Veterinary Services
970-494-7291

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), Veterinary Services Integrated Surveillance Modules (VSISM). VSISM is an enterprise-level (business-wide) animal health and surveillance electronic information management system. It provides an electronic means of data input, data transmission, data storage, and data reporting. This system 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 annual assessment documents update.

Overview

The VSISM is an animal health and surveillance system which provides enterprise-level surveillance and animal health program data for numerous species and diseases to facilitate the detection, management, prevention, investigation, control and eradication of animal diseases.

The VSISM maintains data on collection site, animal, and specimen information, as well as conditions to test for on the specimens, depending on the stream and condition of interest.

The VSISM supports the Veterinary Services 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.

The VSISM 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 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?

2 Employee information – VSISM maintains Name, contact information for collector, submitter, owner, designated epidemiologist

3 Other information – VSISM 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 Physical location of a business or animal herd/flock.

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

Information for VSISM is by collected state or federal staff from people who own or operate:

- Clinic
- Exhibition
- Laboratory
- Market/Concentration Point

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

The purpose of the VSISM system is to allow animal health officials to effectively manage animal disease, pest, and surveillance programs. In the event there are non-negative results for a disease, it may instigate a Foreign Animal Disease (FAD) investigation. Effective management of a FAD depends on traceability and when tracing animals to locations, information on the owners or contacts for that location are needed. Similarly, it may be necessary to contact the person who collected the samples. In both cases, contact information for such persons is retained in VSISM.

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. Information is collected and entered in the application by Federal employees and cooperating State employees directly or based on information on forms. The information is entered directly into the VSISM application by a state or federal employee entering information provided in person, over the phone, in an email, or letter by a producer. Members of the public do not access system to enter data themselves. Data is input by authenticated state and federal employees.

1.5 How will the information be checked for accuracy?

Data collected from customers, USDA sources and non-USDA sources is verified for accuracy, relevance, timeliness, and completeness by USDA and state employees at the time the data is collected. These employees are responsible for the review and accuracy of the data. Verification of data records occurs on an as-needed basis. Persons' address information only provides value during the lifecycle of the laboratory testing process and is not validated beyond the time of collection. Also, there are limited systematic data entry constraints to ensure entry completeness and acceptable values.

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 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 PII data collected from the public and employee business contact, as identified in Section 1.1 above, was the primary privacy risk identified in the PTA. USDA APHIS, including the VS Executive Team, Centers for Epidemiology and Animal Health (CEAH), and State Veterinarians are all responsible for protecting the privacy rights of the employees and other persons identified in the VSISM 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 cyber security Program Manager, 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.
- User access is restricted within the system to relevant data to only a limited dataset is available to a user based on the state for which the individual works. 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 system security awareness training on an annual basis, which mitigates through user education on what is privacy information and how it is protected, and outlines responsibility and accountability for collecting accurate information and ensuring such information is not disclosed with 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 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.

State Veterinarians and State Animal Health officials, as co-owners of the data, have the discretion to share information stored in the VSISM 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.

Certain disease information reported by State and/or Federal employees is recorded in VSISM. These reports are then summarized by APHIS in reports to the (OIE) Office International des Epizooties (World Organization for Animal Health). No 'customer', 'employee' or 'other' private information is published or distributed to OIE.

The Center for Epidemiology for Animal Health (CEAH) and the Commodity Health Centers have agency responsibility for reporting surveillance and program management activities on a nationwide basis. The CEAH and the Commodity Health Centers have direct access to the VSISM data and provide and publish summaries to the public and our trading partners.

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

VSISM data is sent to VS Data Integration Services (a component of the APHIS Marketing Regulatory Services Amazon Web Service General Support System (MRP AWS GSS)) to integrate data with other VS data sources for performing mission critical analysis of surveillance data. Aggregated data is used to produce summary reports for stakeholders via PDF or Tableau. VSISM data is processed and analyzed using tools in VS DIS.

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

VSISM does not use commercial or publicly available data.

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.

- VSISM 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 the VSISM application.
- 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.
- The VSISM application limits access to relevant information and prevents access to unauthorized information through role-based access.
- All users receive security basics 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 VSISM application 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)?

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 contact information, 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/collectors and

premises/animal owners, and premises identification numbers. The benefit of having that data available for premises backtracking and other trending information during an emergency overrides any risk of unauthorized disclosure. All records will be retained while VS awaits NARA disposition and retention scheduling. VSISM maintains information in a secure manner and will dispose of information per APHIS Directive 3440.2 and approval NARA disposition authority.

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?

There is minimal sharing of VSISM data. Specifically, data in VSISM is shared with the USDA Office of the Chief Information Officer's Data Lake environment for Tableau visualization.

4.2 How is the information transmitted or disclosed?

Data is transmitted to the OCIO Enterprise Tableau using secure connections and protocols on a trusted network.

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.

Data exfiltration or loss via interception while in transit is the primary risk associated with the internal data sharing. Data interception by bad actors is mitigated by ensuring the data is transmitted using secure protocols and encrypted connections. Data Loss is mitigated by the USDA Enterprise level Data Loss Prevention solution, which monitors the network for sensitive data on the network or leaving the network via unapproved pathways.

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 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;
- When a record 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 order issued pursuant thereto, disclosure may be made to the appropriate agency, whether Federal, foreign, State, Tribal, local, or other public authority responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutive responsibility of the receiving entity;
- (4) 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 (c) the United States Government, is a party to litigation or has an interest in such litigation, and USDA determines that the records are 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 that is compatible with the purpose for which USDA collected the records;
- (5) 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 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;
- (6) 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;

- (7) 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;
- (8) To contractors their agents, grantees, experts, consultants, and other performing or working on a contract, service, grant, cooperative agreement, or other assignment for the USDA, when necessary to accomplish an agency function related to this system of records. Individuals providing information under this routine use are subject to the same Privacy Act requirements and limitation on disclosure as are applicable to USDA officers and employees;
- (9) To a Congressional office in response to an inquiry from that Congressional Office made at the written request of the individual about whom the record pertains; and
- (10) To the National Archives and Records Administration or other Federal Government agencies pursuant to records management inspections being 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.

Yes. Where the USDA controls the personally identifiable information in the VSISM; 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. The actual sharing to the external source is done by the USDA APHIS Privacy Act Office in the Legislative and Public Affairs (LPA) Branch.

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 byproduct of external is the sharing 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 VSISM. 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 Information Security Branch. Further, the actual release of the data is done by the Legislative and Public Affairs Branch, where the data is triple-checked before it is released to the external point of contact

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.

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

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

There is no Privacy Act Statement required for the VSISM system as it is only utilized by USDA personnel. An effort is underway to update the forms used to collect PII from the public by all of VS to add a Privacy Act Statement. That is separate from the VSISM application.

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

Yes. In order to participate in the program individuals must provide information. When choosing to participate, individuals must provide certain information in order to receive animal health services from APHIS.

Also, 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.

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 use of the information will be noted in the routine uses of the SORN.

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.

There is no Privacy Act Statement required for the VSISM system as it is only utilized by USDA personnel. An effort is underway to update the forms used to collect PII from the public by all of VS to add a Privacy Act Statement. That is separate from the VSISM application.

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. Request 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, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

Customers can contact the APHIS or State office where they first provided the information and request correction of inaccurate or erroneous information. If data provided in response to a FOIA request is found to be inaccurate, the requestor is

directed by the APHIS Privacy Act Officer to request correction by contacting the Freedom of Information Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

Through the Privacy Act Statement, as well as through the SORN.

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

N/A.

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

The primary risk associated with the redress process is delayed response or no response from the APHIS Privacy Office when request is made to correct an individual's personally identifiable information. APHIS VS mitigates this risk by updating an individual's privacy data upon receipt of request from the owner or notification from the APHIS Privacy Office.

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 VSISM 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 VSISM 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. Password controls, procedures, responsibilities and policies follow USDA departmental standards.

8.2 Will Department contractors have access to the system?

Customer Experience Center (CEC) and VS IT Helpdesk contractors have access to the system to manage user accounts.

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

All individuals provided access to the VSISM application are required to complete annual Information Technology (IT) Security Awareness Training and must sign APHIS Rules of Behavior form prior to receiving access to the information system. VS system owners and technical staff are required to complete Protecting PII training each year.

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

Yes. A renewal of Authority to Operate was granted 5/22/2021.

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

Auditing measures are applied in accordance with FIPS 199/200 Moderate Baseline Security Controls. Some of the technical safeguards for VSISM 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 create, modify, delete, old, and new values are audited at the field level. 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 (VSISM roles).

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?

VSISM uses a defense in depth approach to protect and ensure the confidentiality and integrity of the customer data. Unauthorized access, unauthorized disclosure or disposal of the data are the risks to this data, and these are mitigated by ensuring the implementation of technical controls such as auditing, access control and system communications; the implementation of operational controls like configuration management, contingency planning, system and security integrity, and the

implementation of management controls such as annual risk assessments, planning and security assessment and authorization, are in place and operating as expected. These controls are explained in NIST Special Publication 800-53Additionally, VSISM sits on the MRP Azure Cloud GSS and inherits additional technical security controls. These controls are part of the cybersecurity framework and are implemented in accordance with NIST Special Publication 800-53 Revision 4. This guidance document lays out the suite of controls that are operational, technical, and management safeguards to be used by information systems to maintain the integrity, confidentiality, and security of federal information systems.

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 USDA APHIS Veterinary Services Integrated Surveillance Modules (VSISM) 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.

This application 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. VSISM 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. VSISM 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. VSISM 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. VSISM 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. VSISM 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. VSISM 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. VSISM 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. VSISM does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

Not applicable. VSISM does not use third party websites or applications.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Not applicable. VSISM does not use third party websites or applications.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Not applicable.

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.

Agency Responsible Officials

NEIL WYMAN
Digitally signed by NEIL WYMAN
Date: 2023.11.21 11:10:51 -07'00'

Neil Wyman
System Owner
Animal Plant Health Inspection Service
United States Department of Agriculture

Date

Agency Approval Signature

Janelle Jordan
Digitally signed by Janelle Jordan
Date: 2023.11.21 17:19:37 -05'00'

Tonya Woods
APHIS Privacy Officer
United States Department of Agriculture

Date

ANGELA COLE
Digitally signed by ANGELA COLE
Date: 2023.11.21 17:51:01 -05'00'

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

Date