Privacy Impact Assessment
VS NITC

- Version: 1.5
- Date: September 26, 2017
- Prepared for: APHIS Veterinary Science National Information Technology Center (VS NITC) Systems

Privacy Impact Assessment for the Veterinary Service National Information Technology Center (VS NITC) System

September 2017

The VS NITC System is comprised of several applications. Currently these applications are:

- Animal Disease Traceability Information System (ADTIS)
- Laboratory Messaging Services (LMS)
- User Fee System (UFS)
- Veterinary Services Laboratory Submissions (VSLS) and
- Veterinary Services Process Streamlining System (VSPS)

This PIA contains the data for all components comprising the VS NITC System. Details for each application are contained under the respective heading.

ABSTRACT-Animal Disease Traceability Information System (ADTIS)

- This Privacy Impact Assessment (PIA) is for the USDA, APHIS, Veterinary Services (VS), Animal Disease Traceability Information System (ADTIS).
- ADTIS supports animal disease traceability activities related to animal identification, movements and locations where animals are managed. It is being implemented by the USDA and state agencies – in cooperation with industry - to enable timely trace back of the movement of diseased or exposed animal. This program helps to ensure rapid disease containment and maximum protection of America's animals.
- This PIA was conducted as part of APHIS continuous monitoring activities.

OVERVIEW-ADTIS

The ADTIS contains three major components; Standardized Premises Information System (SPIS), Premises Allocator/ Repository, and the Animal Identification Management System (AIMS). Additionally, the Animal Health Event Repository (AHER) is a data mart/warehouse-like data store for a subset of the application data. Software has been deployed to support premises identification and animal identification. Premises identification process involves assigning a unique seven-character identifier premises identification number (PIN) to premises in the United States (US) where livestock are managed or held (e.g., for marketing, processing, etc.). There are in excess of two million premises in the US. USDA provides the ADTIS to State and Tribes that elect to utilize the information systems as part of their animal disease traceability plan. The basic operational characteristics of the modules are explained below.

(1) Standardized Premises Information System (SPIS) – an application offered free to states enabling them to manage their state premises identification activities. Approximately 50 States, 5 tribes and 2 territories use ADTIS, their own system or a third party system. SPIS has data tables of its own, used to store data of interest to State animal health officials. SPIS communicates with the Allocator when attempting to retrieve a PIN. SPIS is a J2EE application with an Oracle backend. The SPIS provides a common, free-for-use system for individual States and Tribes to manage locations (premises) that raise or hold livestock as part of their local animal disease traceability plans. The data is segregated on a State-by-State basis. The system provides separation at the State level, providing the ability for each state to manage their data independently of other States. Within each State, users register an account

(providing business information), and user contact information. These on-line users can then obtain one or more PIN for their account. Through the premises identification process, the system connects to the Allocator to generate/provide the PIN.

(2) Premises Allocator/ Repository. The premises allocator, a Java 2 Platform, Enterprise Edition (J2EE) application is used to validate addresses, assign computer-generated PINs to valid addresses, and transfer premises data between a state system and the national repository. The allocator also connects to commercial addresses databases (i.e. US Post Office, and TeleAtlas) to check the validity of addresses. The allocator is accessed via Application Programming Interface (API) by other internal and external modules. In addition, the Allocator provides search, create, and modify features. The premises repository, maintains Oracle tables with for premises records and the core data elements. Data inserts, updates, queries and delete functions mostly occur via the Allocator although some direct query functionality exists between the DMC and the NPIR.

(3) Additionally, the Data Management Center (DMC) is a utility that supports the administration of PINs, in particular when the business rules for a valid address for a location is not met. The DMC is a J2EE application that was originally built to support ADTIS helpdesk personnel in researching addresses that will not validate against commercial databases, to run various reports against the Premises Allocator, and to support other access and general management of the premises repository. With recent security upgrades, selected state animal health officials can also have access to the DMC to perform these functions against the data for their state. The DMC interfaces with both the allocator and the national repository.

(4) Animal Identification Management System (AIMS) – Basic to identification is assigning and maintaining official unique animal identification numbers. AIMS is designed to facilitate order and delivery of physical animal identification devices to premises locations and to maintain other animal events such as animal movements.

(5) The Animal Health Event Repository (AHER) is a data mart/warehouse repository that receives information from most of the other VS data stores.

1 Characterization of the Information ADTIS

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?

General contact information is recorded in the SPIS on individuals that are associated with a premises; specifically, name, address, company name, contact numbers, and e-mail. All other information is in regards to the animals in the possession of the customers and only collected during a disease or other health event. Such animal information collected includes: specific systems that provided the information (i.e., premises data, animal ID manufacturers, and animal tracking institutions), Premises ID, Animal ID, date of event, event type, breed and sex.

The information contained in the system is based on the tracing of animals. Personal information of individuals is only used for verification and contact purposes for the goal of tracing and containment of diseased or exposed animals.

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

The sources of information are:

- State Boards of Animal Health and/or Departments of Agriculture and/or agents as assigned by the State and Tribal authorities.
- Manufacturers of official identification devices and device managers provide records of shipments of official identification devices from their location to other premises.
- Animal identification numbers used in the administration of disease programs that utilize the Mobile Information Management System (MIMS) are uploaded to AIMS.

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

(1) Information is used by Federal and State animal health officials during a foreign animal disease (FAD) outbreak, bioterrorism, or other animal health emergency to contain and respond to the emergency event. Specifically, the information aids in the traceback and or trace forward of exposed and potentially exposed animals.

(2) Information will be referred to the appropriate agency whether Federal, State or local, charged with the responsibility of investigating or prosecuting a violation of law or enforcing or implementing a statute, rule, regulation or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by rule, regulation or order issued pursuant thereto.

(3) Information will be disclosed to the Department of Justice for use in litigation when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, where the agency determined that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determined that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

(4) Information will be disclosed in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee, or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

Information will be disseminated to solicit feedback from federal and state animal health officials within the system on emergency preparedness guidelines and the system itself for the purpose of educating and involving the federal and state animal health officials in program development, program requirements, and standards of conduct.

1.4 How is the information collected?

States and Tribes that elect to use the SPIS obtain the premises information from producer on forms, and then the information is entered into the SPIS by individuals, the employee, or the State and Tribes sets the SPIS to enable on-line use by producers so they can enter the

information directly to the SPIS via the internet. The information on official identification numbers are entered through on-screen entries or computer to computer through established web services by official identification device manufacturers, managers and animal health officials. The Mobile Information Management System (MIMS) provides records on animal identification obtained through the administration of animal disease programs.

1.5 How will the information be checked for accuracy?

Data is collected from States, Tribes, Animal Health Officials (AHO), and ID tag manufacturers. The premises allocator has many safeguards to ensure the no more than one PIN is issued to a location which is critical to the integrity of the traceability data.

Premises data collected in the system is verified by the State AHOs or their agents. ADTIS currently requires all premises addresses to be validated by one of three databases (ZP4, Tele Atlas, or Google) or go through the exception process. The exception process is a published Standard of Procedure (SOP) that is designed to verify driving directions (using an electronic map) and insuring they match with the provided Global Positioning Satellite (GPS) coordinates. Exception reports are generated if there is data that contradicts the completeness of existing information in the system.

AINs are allocated to approved official identification devices and their uniqueness is also controlled. Records submitted by users to AIMS must have a valid PIN or Location Identifier (LID).

The system will not allow the submission of data unless it is complete and verified. State AHOs must verify the information prior to entering the data into the system. The system will not allow the data to be stored without providing all the required data.

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.

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 customer personally identifiable data is the primary privacy risk as identified in the Privacy Threshold Analysis (PTA0. USDA APHIS, including the VS Management Team, is all responsible for protecting the privacy rights of the customers and

employees identified in the ADTIS as required by applicable State and Federal laws. Specific mitigation activities are:

- Appropriate Level 2 eAuthentication logon credentials by users and/or database authentication are used to gain access to the system. The eAuthentication access is monitored by USDA officials to ensure authorized and appropriate use of data. Additionally, user roles are established to ensure users have access to certain types of data based on their roles and need to access certain types of data in this system.
- User access is restricted within the system to relevant data. 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. A user may be restricted to the information only pertaining to their particular state while others may have access to multiple sets of data.
- All organizational users are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training

At the login screen of the application the warning banner must be acknowledged before users are allowed access.

2 Uses of the Information ADTIS

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 information collected on individuals is in relation to the tracing of animals, the location of animals currently in their possession and the history of locations for those animals and animals that may have been co-mingled with the animal of interest.

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

Microsoft Excel, XML and text reports are currently used to analyze the data collected in ADTIS.

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

ADTIS currently requires all premises addresses to be validated by one of three databases: ZP4 or Tele Atlas.

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.

- Access to ADTIS is controlled by the USDA eAuthentication system and/or database authentication.
- The application contains security measures to limit access to relevant information and prevents access to unauthorized information.
- At the login screen of the application the warning banner must be acknowledged before users are allowed access.
- Security controls within the application are reviewed by independent assessors every year, in order to verify that they are operating as expected.
- Access to personal information is restricted to individuals with a need to know in order to perform functions associated with their job.
- All organizational users are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training.

Failure to comply with Rules of Behavior could result in strict disciplinary action, including termination or other adverse action that is deemed appropriate.

3 Retention ADTIS

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 data is retained indefinitely within the application.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention period approval is pending. The VS officials are taking the necessary action to ensure that the records retention period is approved by NARA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The data is monitored by the USDA ADTIS team. Because of the constant change and update of information, the data is continuously monitored by system users who regularly review the data by running reports and queries. This type of review and monitoring ensures the information in the system is accurate and up to date. Safeguards are in place to ensure that data is restricted to only authorized individuals. ADTIS maintains this information in a secure manner.

4 Internal Sharing and Disclosure ADTIS

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?

ADTIS Personnel: The only members with direct access to the system will be those internal to APHIS who has been granted access to the system. These will include System Administrators and Database Administrators, in addition to assigned APHIS personnel responsible for auditing and querying data in the application.

4.2 How is the information transmitted or disclosed?

The information is transmitted either via direct access by the user or by a system to system secure process. Access to the system and data is based on the role of the user. Each user is given permissions within the ADTIS based on the need to obtain or update the information.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Unauthorized disclosure of personal information is the primary privacy risk to information shared internally to APHIS. These risks are mitigated through ADTIS and National Information Technology Center (NITC) General Support Services (GSS) security controls as delineated in the current ADTIS System Security Plan.

User access is restricted within the system to relevant data. 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. A user may be restricted to the information only pertaining to their particular state while others may have access to multiple sets of data.

5 External Sharing and Disclosure ADTIS

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?

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, records maintained in the system may be disclosed outside USDA as follows:

(1) To Federal and State animal health officials to contain and respond to a foreign animal disease event, bioterrorism, or other animal health event. Use of the information contained in the ADTIS aids in the determination of the origin of an incident of an animal disease and in the location of exposure and other potentially exposed animals;
(2) To Federal and State animal health officials within the system to obtain feedback regarding the ADTIS effort and emergency preparedness guidelines; to educate and involve them in program development, program requirements, and standards of conduct; and to validate such information;
(3) To the appropriate agency, whether Federal, State, local, or foreign, charged with responsibility of investigating or prosecuting a violation of law or of enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and either arising by general statute or particular program statute, or by rule, regulation, or court order issued pursuant thereto;
(4) To the Department of Justice when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, in litigation, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by

the Department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which the records were collected;

(5) For use in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee, or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected

(6) To appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the agency has determined that as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, a risk of identity theft or fraud, or a risk of harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(7) To contractors and other parties engaged to assist in administering the program. Such contractors and other parties are bound by the nondisclosure provisions of the Privacy Act. This routine use assists the agency in carrying out the program, and thus is compatible with the purpose for which the records are created and maintained;

(8) To USDA contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends, or anomalies indicative of fraud, waste, or abuse. Such contractors and other parties are bound by the nondisclosure provisions of the Privacy Act; and

(9) To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine

use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Where the Department controls the personally identifiable information in the ADTIS; use of that information will be governed by an appropriate routine use in a System of Record Notice (SORN). Where the ADTIS information is controlled by State authorities, the legal mechanisms employed are per state information security law and regulation. APHIS VS works with State authorities on data protection through written agreements, such as Memoranda of Understanding, Interconnectivity Agreements, and Cooperative Agreements.

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

Current information is shared through role-based access within the application and to reports generated by the application processes.

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

Unauthorized disclosure of personal information is the primary privacy risk to information shared internally to APHIS. These risks are mitigated through ADTIS and APHIS Enterprise Infrastructure (AEI) & NITC GSS security controls as delineated in the current ADTIS System Security Plan.

6 Notice ADTIS

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.

ADTIS SORN

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

A System of Record Notice has been published in the Federal Register for ADTIS

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

The States and Tribes are not required to obtain PINs for livestock locations. However, if they elect to use PINs in their traceability system, the required data elements must be entered into the SPIS. While the use of AIN devices is the choice of the producer and/or owner of the livestock, the reporting of the official numbers on the AIN devices using the PIN or LID is required. Therefore, when records are entered into ADTIS, the required fields must be provided by the user.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The data are treated uniformly for all submitters. Once the information is submitted it is subject to all routine uses.

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

The System of Record Notice is the official notice. The States and Tribes administer the identification of locations, thus are responsible for informing the individuals of what information is being provided to the ADTIS.

7 Access, Redress and Correction ADTIS

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

7.1 What are the procedures that allow individuals to gain access to their information?

Any individual may obtain information from a record in the system that pertains to him or her. Requests for hard copies of records should be in writing, and the request must contain the

requesting individual's name, address, name of the system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

States and Tribes update the premises contact information on the SPIS. Additionally, users are required to submit a request for Premises address updates to the ADTIS Help Desk.

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

The States and Tribes update premises contact information by routine renewal-type notices. For those areas within the application where the user does not have update permission, the user contacts their respective State Animal Health Administrator, who, in turn, contacts the ADITS Help Desk for assistance.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232. Include the reason for

contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

The primary risk associated with the redress process is the loss of the written request. If the written request is mailed, the U.S. Post Office handling practices are the primary mitigations to data loss. Hand carried requests by the requester are the requesters responsibility to protect. Once received by the VS the requests are treated as sensitive material in accordance with the formal redress methods.

8 Technical Access and Security ADTIS

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 ADTIS 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 ADTIS information are further controlled through electronic role-based access. Users must have a government issued login and password that is controlled and managed either at the Veterinary Services Regional or Area 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?

VS IT contractors are provided access only as needed to perform the requirements of a given contract. Contractors are involved in the design and development of the ADTIS. Privacy clauses are included in the associated contracts. Contractors will not be involved in the production support of the application.

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 the ADTIS 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.

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

The ADTIS has completed Certification and Accreditation and has an Authority to Operate that expires in July 2017.

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

Formal auditing measures for the ADTIS will include security assessments performed by APHIS at least annually and independent security assessments performed in support of Certification and Accreditation efforts. The independent assessments will be performed per the timeframe of ADTIS Re-certification.

As to technical safeguards:

- The ADTIS is continuously monitored in several different ways. NITC performs a monthly scan of systems to identify possible threats. The vulnerabilities identified are required to be remediated by the responsible parties. Security related incidents are reported to the Information System Security Manager (ISSM) which in turn requires an investigation. Also, all computers located within APHIS are required to have USDA-approved antivirus software installed. Once installed, the configuration is setup to receive updates twice weekly and to scan the machine daily. In addition, APHIS Customer Service Representatives have configured Windows Update to run on all machines for which they are responsible.
- NITC scans all systems at least every thirty days. This is conducted through the NITC/VS Reimbursable Agreement and results provided to the VS Program Support Services staff.
- Operational technical safeguards to prevent data misuse begin with access control. ADTIS employs SSL encryption to protect data during transmission. Access to ADTIS information is protected by role-based access which is managed by the network firewall, eAuthentication, and the ADTIS application. Users must have a government issued login and password that is controlled and managed either at the Veterinary Services. Password controls, procedures, responsibilities and policies follow USDA departmental standards. At most sites, responsibility and scope of data access is defined by users' job descriptions. Policy dictates that a user may 'self-nominate' themselves for access. Requests for access must be approved by a supervisor or APHIS authorizing official.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what

privacy risks were identified and how do the security controls mitigate them?

Unauthorized disclosure of employee and other personnel information is the primary privacy risk to information shared both internally and externally to the USDA. This risk is mitigated through technical and procedural information security controls levied on internal and external holders of ADTIS data. ADTIS and NITC GSS technical security controls are delineated in the current ADTIS System Security Plan.

9 Technology ADTIS

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 ADTIS is an operational major application (MA). The data in the Animal Disease Traceability Information System (ADTIS), is used to support to its mission and responsibilities authorized by the Animal Health Protection Act (7 U.S.C. 8301 et seq.). APHIS, in cooperation with States, Tribes, and producers, safeguards U.S. animal health through a variety of activities including disease control. One important part of disease control is animal disease traceability. The animal disease traceability effort is a flexible yet coordinated approach that embraces the strengths and expertise of States, Tribes, and producers and empowers them to find and use the traceability approaches that work best for them. Information systems are crucial to support the traceability of farm-raised livestock and poultry that move interstate that might have disease or be exposed to a disease.

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

The ADTIS application does not employ technology that may raise privacy concerns.

10 Third Party Websites/Applications ADTIS

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

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed

Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

OMB M-10-22 and OMB M-10-23 have been distributed by APHIS VS.

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

Data from ZP4 or Google Maps, are used in ADTIS to validate premises addresses.

10.3 What personally identifiable information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

The type of PII received is mapping coordinates only. No other information is exchanged.

10.4 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

Only mapping coordinates are made available and this information is used to validate existing information.

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?

The mapping coordinates are stored within the ADTIS database and is controlled by the same technical measures and safeguards specified in 8.5.

10.6 Is the PII that becomes available through the agency’s use of 3rd party websites and/or applications purged periodically?

The mapping coordinates are retained as stated in 3.1.

If so, is it done automatically?

The mapping coordinates are retained as stated in 3.1.

If so, is it done on a recurring basis?

The mapping coordinates are retained as stated in 3.1.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Only authorized users have access to records within ADTIS.

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?

The information will be shared as stated in section 4.1 and 5.1.

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)?

The information is covered under the existing ADTIS SORN and no modifications to the SORN are required.

10.10 Does the system use web measurement and customization technology?

ADTIS does not use web measurement or customization technology.

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

ADTIS does not use web measurement or customization technology.

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?

ADTIS does not use web measurement or customization technology.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

ADTIS does not use web measurement or customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

ADTIS does not use web measurement or customization technology.

ABSTRACT-Laboratory Messaging Services (LMS)

- The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:
- This Privacy Impact Assessment (PIA) is for the USDA, APHIS, Veterinary Services (VS), Laboratory Messaging System (LMS) IT System.
- LMS is an enterprise-level (business-wide) information system that forms part of a nationwide strategy to coordinate the work of participating veterinary diagnostic laboratories providing animal health surveillance and testing services for APHIS.
- This PIA was conducted as part of APHIS continuous monitoring activities.

OVERVIEW-LMS

The Laboratory Messaging System (LMS) forms part of a nationwide strategy to coordinate the work of participating veterinary diagnostic laboratories providing animal health surveillance and testing services for APHIS.

At the Federal level, the U.S. Department of Agriculture's (USDA) National Veterinary Services Laboratories (NVSL) serves as the national veterinary diagnostic reference and confirmatory laboratories. The State/university laboratories in the LMS perform routine diagnostic tests for endemic animal diseases as well as targeted surveillance and response testing for foreign animal diseases.

Networking these resources provides an extensive infrastructure of facilities, equipment, and personnel that are geographically accessible no matter where disease strikes. The laboratories have the capability and capacity to conduct nationwide surveillance testing for the early

detection of an animal disease outbreak. They are able to test large numbers of samples rapidly during an outbreak and to demonstrate freedom from disease after eradication.

It is a “Major Application” with a FIPS-199 classification of “Moderate”.

1 Characterization of the Information LMS

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?

The information collected includes: name, address information, location address or geocode for point of sample collection, laboratory name, laboratory address, test results, and patient (animal) information.

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

Information in this system comes primarily from - the LMS laboratories.

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

Test results for multiple diseases including Avian Influenza, Swine Enteric Coronavirus Disease, Vesticular Stomatitus Virus, Swine Influenza Virus, African Swine Fever, Foot Mouth Disease, and others are transmitted over secure http in an HL7 message, or loaded by spreadsheet by federal users. Rhapsody messaging services is the gatekeeper for incoming data routing it or rejecting it as appropriate. Surveillance analysts currently have read only access to the Oracle data for analysis and reporting. System integration is as follows:

EMRS2: Centerprise pull of data into EMRS2 from the LMS database.

VSLS: Rhapsody routes data intended for VSLS at the point of receipt. VSLS has no connection to the LMS database.

SCS: Information will be sent over secure http using an xml schema defined by the SCS vendor. No direct database connection will exist.

1.4 How is the information collected?

The LMS labs securely (via HTTPS) send XML result messages in HL7 format to the (Rhapsody Messaging Server).

1.5 How will the information be checked for accuracy?

The following steps are taken for data verification at the LMS laboratory level, as part of their Quality Management Systems:

- Submission form received and data entered by receiving technician.
- Testing is performed and documented by lab technician.
- Test results are entered into the system by a data entry clerk or lab technician.
- Lab Manager checks for accuracy, by reviewing submission documents and tests result document that were entered into the system by a clerk or technician.
- Case Coordinator verifies completeness of data by reviewing documents and/or taking reasonable person approach.

Accuracy verification: rules are enforced to confirm that the correct patient animal species and specimen types are tested for specific animal health programs, and that the correct test result type is reported for specific animal health programs.

Relevance verification: rules are enforced to confirm that the laboratory that is reporting test results is officially registered in the LMS laboratory registry.

Completeness verification: rules are enforced for required data elements to be submitted with each messaged test result.

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

Laboratory Messaging System (LMS) maintains the collection pursuant to its missions and responsibilities authorized by the:

- Animal Health Protection Act (7 U.S.C. 8301–8317);
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Pub. L. 107–188);
- Homeland Security Presidential Directive-7;
- Homeland Security Presidential Directive-9.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Collection of inaccurate data and unauthorized disclosure of customer personally identifiable data are the primary privacy risk as identified in the PTA. USDA APHIS, including the VS Management Team, NVSL, and participating LMS laboratories are all responsible for protecting the privacy rights of the users identified in the LMS program. Specific mitigation activities are:

- All access to the data in the system is controlled by an authorization process. An APHIS point of contact or supervisor must identify (authorize) what functional roles that individual needs in the LMS IT system.
- Data is transmitted from the LMS laboratories to Rhapsody in a secure manner.
- The application limits access to relevant information and prevents access to unauthorized information. Access to the data is controlled by roles and privileges assigned through the Oracle Database in which the data is housed.
- All organizational users are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training.
- Data validation and verification is performed on the data to mitigate the risk of inaccurate data being collected and stored.

2 2 Uses of the Information LMS

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.

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

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

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

The data is analyzed using SQL, or exported for analysis in SAS. Systems that consume the data such as VSLS and EMRS2 also allow users to view and analyze the data as well as edit

it. A chain of custody is maintained so that such edits to results can be traced back to the original data received and persisted in the LMS repository.

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

The LMS IT System 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.

- Security controls within the application are reviewed internally each year, and by independent assessors every three years, in order to verify that they are operating as expected.
- Access to personal information is restricted to individuals with a need to know in order to perform functions associated with their job.
- All organizational users are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training. Failure to comply with Rules of Behavior could result in strict disciplinary action, including termination or other adverse action that is deemed appropriate.

3 Retention LMS

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

3.1 How long is information retained?

Electronic records are currently retained within the system for 50 years. Electronic records stored on LMS IT System computer hard drives are backed up nightly. Incremental and full system tape backups are retained for one month. Backup media is regularly sent to an off-site backup storage facility for contingency purposes.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

This is in progress. The LMS IT System is taking necessary action to ensure that the MRP 400 is completed and submitted to NARA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Preservation of data integrity and accuracy is primary risk if data is retained in excess of its official records retention schedule. To mitigate this risk data is maintained and disposed of in accordance with APHIS records retention schedules that are applicable to the system. Safeguards are in place to ensure that data is restricted to only authorized individuals. Personally Identifiable Information (PII) is limited to submitter's name, mailing address and phone number. LMS maintains this information in a secure manner.

4 Internal Sharing and Disclosure LMS

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?

Surveillance analysts have direct access to the data. The data is consumed by other systems where it is available to users but not modifiable. These systems are Veterinary

Services Laboratory Submissions (VSLS) and Emergency Management Response System (EMRS2).

4.2 How is the information transmitted or disclosed?

Incoming information is transmitted over secure http in an HL7 message, or loaded by spreadsheet by federal users. Rhapsody messaging services is the gatekeeper for incoming data routing it or rejecting it as appropriate. Surveillance analysts currently have read only access to the Oracle data for analysis and reporting. System integration is as follows:

EMRS2: Centerprise pull of data into EMRS2 from the LMS database.

VSLS: Rhapsody routes data intended for VSLS at the point of receipt. VSLS has no connection to the LMS database.

SCS: Information will be sent over secure http using an xml schema defined by the SCS vendor. No direct database connection will exist.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Unauthorized disclosure of personal information is the primary privacy risk to information shared internally to APHIS. These risks are mitigated through LMS and NITC GSS security controls through general and privileged access control policies, including required authentication and authorization; annual user access reviews; and audit monitoring and review.

5 External Sharing and Disclosure LMS

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?

(1) To Federal and State animal health officials to aid in containing and responding to a foreign animal disease outbreak, bioterrorism, or other animal health emergency;
(2) To cooperative LMS laboratories, Federal, State, and local government officials, employees, or contractors, and other parties engaged to assist in administering the program. This routine use assists the agency in carrying out the program, and thus is compatible with the purpose for which the records are created and maintained;
(3) To responsible Federal and State animal health officials to evaluate response and surveillance activities;
(4) To Federal and State animal health officials within the system to disseminate information and solicit feedback on emergency preparedness guidelines and the system itself for the purpose of educating and involving these officials in program development, program requirements, and standards of conduct;
(5) To the appropriate agency, whether Federal, State, local, or foreign, charged with responsibility of investigating or prosecuting a violation of law or of enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and either arising by general statute or particular program statute, or by rule, regulation, or court order issued pursuant thereto;

(6) To the Department of Justice when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, in litigation, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which the records were collected;

(7) For use in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee, or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected;

(8) To appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, a risk of identity theft or fraud, or a risk of harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(9) To contractors and other parties engaged to assist in administering the program. Such contractors and other parties will be bound by the nondisclosure provisions of the Privacy Act. This routine use assists the agency in carrying out the program, and thus is compatible with the purpose for which the records are created and maintained;

(10) 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

(11) To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Where the Department controls the personally identifiable information in the LMS IT System; use of that information will be governed by an appropriate routine use in a SOR Notice. Where the LMS laboratory information is controlled by State or University authorities, the legal mechanisms employed are per state information security law and regulation. APHIS VS works with State authorities on data protection through the use of NDAs, ISAs, MOUs and other agreements. APHIS does not share PII outside of the department for CSF or AI testing that is encompassed in the LMS IT System.

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

Current information is shared through direct role-based access within the application. Submitting LMS laboratory officials are only able to view the data which they have submitted. No other parties outside of the department are able to view raw, submitted testing data.

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

Unauthorized disclosure of personal information is the primary privacy risk to information shared externally to APHIS. These risks are mitigated through VSPS and NITC GSS security controls through general and privileged access control policies, including required authentication and authorization; annual user access reviews; and audit monitoring and review.

6 Notice LMS

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.

LMS SORN (previously named NAHLN)

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

A System of Record Notice has been published in the Federal Register for the Laboratory Messaging System under SORN APHIS-5.

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

No, if information is required then the user must provide the requested information or they may choose not to perform testing for APHIS under the LMS system.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The data are treated uniformly for all submitters. Once the information is submitted it is subject to all routine uses.

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

The System of Record Notice is the official notice. No information is collected without an individual's awareness. At the LMS laboratory level, the laboratory chooses to provide data into the LMS IT System. The LMS laboratory is responsible for notifying private (non-Federal or State) submitters that their sample and test result may be selected to be part of an APHIS national surveillance program.

7 Access, Redress and Correction LMS

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

7.1 What are the procedures that allow individuals to gain access to their information?

Any individual may obtain information from a record in the system that pertains to him or her. Requests for hard copies of records should be in writing, and the request must contain the requesting individual's name, address, name of the system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

LMS attempts to strongly preserve the information exactly as transmitted by the laboratories. Editing of that data or corrections is done in external systems maintaining a chain of custody to the unedited record, or by laboratories messaging updated information. Responsibility for validation of the data rests in the business community who have the professional knowledge to properly interpret the data received.

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

Individual data is not maintained in LMS. Submitter name, address and phone number may be sent, and inaccuracies in that data are corrected in external systems or by the lab sending a new message.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

The primary risk associated with the redress process is the loss of the written request. If the written request is mailed, the U.S. Post Office handling practices are the primary mitigations to data loss. Hand carried requests by the requester are the requesters responsibility to protect. Once received by the VS the requests are treated as sensitive material in accordance with the formal redress methods. The information in LMS comes directly from the LMS Laboratories. It is the responsibility of these labs to correct and inaccurate data upon notification.

8 Technical Access and Security LMS

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?

The LMS IT system is subject to management, operational, and technical controls. Such controls include role-based access based on assigned responsibility for animal health; data encryption during transmission; configuration management; and physical and environmental protections. Each user's access is restricted based the user's role, laboratory where employed, and region of assigned responsibility for animal health.

8.2 Will Department contractors have access to the system?

VS IT contractors are provided access only as needed to perform the requirements of a given contract. Contractors are involved in the design and development of the LMS. Privacy clauses are included in the associated contracts and all contractors must complete a background checks per Department Human Resource policies. Contractors will not be involved in the production support of the application.

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

All users who are provided access to the LMS IT application are required to complete annual USDA Information Technology (IT) Security Awareness Training and must sign APHIS Rules of Behavior form prior to receiving access to the information system.

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

The LMS IT System received an Authority to Operate in June 2014.

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

Formal auditing measures for the LMS IT System will include security assessments performed by APHIS at least annually and independent security assessments performed in support of Certification and Accreditation efforts. The independent assessments will be performed per the timeframe of LMS Re-certification.

As to technical safeguards:

- The LMS IT System is continuously monitored in several different ways. AEI GSS and NITC perform a monthly scan of systems to identify possible threats. The vulnerabilities identified are required to be remediated by the responsible parties. Security related incidents are reported to the ISSM which in turn requires an investigation. Also, all computers located within APHIS are required to have USDA-approved antivirus software installed. Once installed, the configuration is setup to receive updates twice weekly and to scan the machine daily. In addition, APHIS Customer Service Representatives have configured Windows Update to run on all machines for which they are responsible.
- NITC scans all systems at least every thirty days. This is conducted through the NITC/VS Reimbursable Agreement and results provided to the VS CIO Technology staff.
- Operational technical safeguards to prevent data misuse begin with access control. The LMS IT System employs SSL encryption to protect data during transmission. Access to LMS information is protected by role-based access which is managed by the network firewall and the LMS IT application. Users must have a government issued login and password that is controlled and managed either at the Veterinary Services headquarters or field offices. Password controls, procedures, responsibilities and policies follow USDA departmental standards. At most sites, responsibility and scope of data access is defined by users' job descriptions. Policy dictates that a user may 'self-nominate' themselves for access. Requests for access must be approved by a supervisor or APHIS authorizing official.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any

information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Unauthorized disclosure of employee and other personnel information is the primary privacy risk to information shared both internally and externally to the USDA. This risk is mitigated through technical and procedural information security controls levied on internal and external holders of LMS data.

9 Technology LMS

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 LMS IT System is an operational major application (MA). The LMS is an information-centered, test result repository. LMS has no user interface. LMS is dependent on the direct, electronic exchange of laboratory testing data between veterinary diagnostic laboratory information systems, centralized messaging routers of VS information systems to support animal health program surveillance and diagnostic testing needs, including those in an animal disease outbreak.

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

The LMS application does not employ technology that may raise privacy concerns.

10 Third Party Websites/Applications LMS

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

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology”

and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

OMB M-10-23 and OMB M-10-22 have been distributed by APHIS VS.

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

The LMS IT System does not use a 3rd party application.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

The LMS IT System does not receive any personally identifiable information from 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?

The LMS IT System does not receive any personally identifiable information from 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?

The LMS IT System does not receive any personally identifiable information from 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?

The LMS IT System does not receive any personally identifiable information from third party websites or applications.

If so, is it done automatically?

The LMS IT System does not receive any personally identifiable information from third party websites or applications.

If so, is it done on a recurring basis?

The LMS IT System does not receive any personally identifiable information from 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?

The LMS IT System does not receive any personally identifiable information from 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?

The LMS IT System does not receive any personally identifiable information from 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)?

The LMS IT System does not receive any personally identifiable information from third party websites or applications.

10.10 Does the system use web measurement and customization technology?

The LMS IT System does not use web measurement or customization technology.

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

The LMS IT System does not use web measurement or customization technology.

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?

The LMS IT System does not use web measurement or customization technology.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

The LMS IT System does not use web measurement or customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

The LMS IT System does not use web measurement or customization technology.

ABSTRACT-User Fee System (UFS)

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- This Privacy Impact Assessment (PIA) is for the USDA, APHIS, Veterinary Services (VS), User Fee System (UFS).
- The UFS is used to provide a unified and automated process to track the user fees collected by Veterinary Services' sites across the nation. .
- This PIA was conducted as part of APHIS continuous monitoring activities.

OVERVIEW-UFS

The Animal and Plant Health Inspection Service's (APHIS) Veterinary Services (VS) program uses the Veterinary Services User Fee System to automate the tracking, collection, and processing of fees due to VS for its services provided at remote offices, import centers, port offices, or the National Veterinary Services Laboratories in Ames, IA. In order to ensure that animals and animal products do not introduce pests or diseases when imported into the United States, the VS program of APHIS performs services related to the importation and exportation of animals, animal products, birds, germ plasm, organisms, and vectors. VS incurs costs associated with inspections and other services, such as the costs of maintaining import centers and quarantine facilities, diagnostic testing, inspectors' salaries, supplies, and other miscellaneous expenses. Any person for whom a service is provided related to the

importation, entry, or exportation of an animal is required to pay for the expenses of such services.

The UFS generates an invoice for the fees, provides a receipt for the user, and tracks the accuracy of expenditures and collections transactions. UFS subsequently provides the billing information to the Marketing & Regulatory Programs Business Services (MRPBS) in Minneapolis, MN and the Office of the Chief Financial Officer—National Finance Center (OCFO-NFC) in New Orleans, LA.

1 Characterization of the Information UFS

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?

The system collects information from citizens that include name, address, phone number, fax number, APHIS credit account number, control/receipt number, fees charged, method of payment and amount paid for services provided by Veterinary Services. For example, fees are collected when importing/exporting animals or animal products.

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

Information is input into the UFS via an electronic APHIS-81 form. A customer may also open an account by completing an APHIS-192 and sending it to Minneapolis where it is input into UFS after being approved by the NFC. Information is also input into UFS from the NVSL Labware Laboratory Information System (LIMS) through a data transfer process.

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

The data is used to assess and collect fees for services provided by Veterinary Services. This includes tracking payment history (i.e., payments made in cash, check, or credit card as well as nonpayment history). It also includes the type(s) of services provided by VS.

1.4 How is the information collected?

The information is collected through data entry directly into the application via the Internet or through completion of OMB approved APHIS forms.

1.5 How will the information be checked for accuracy?

Data that is collected from customers who are applying for an APHIS credit account is verified by the APHIS MRPBS Financial Management Division (FMD) office in Minneapolis. In addition, customers may verify that amount charged and collected by APHIS is accurate by reviewing the hardcopy of the APHIS 81 that they are provided at the time of services.

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

- 9 CFR 130.2 User Fees
- Debt Collection Act of 1982 (31 U.S.C. 3701 et seq.),
- Debt Collection Improvement Act of 1996 (31 U.S.C. 3711 et seq.),
- Food, Agriculture, Conservation and Trade Act of 1990 (Public Law 101-624),
- Animal Health Protection Act (7 U.S.C. 8301 et seq.).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Collection of inaccurate data and unauthorized disclosure of customer personally identifiable data are the primary privacy risks as identified in the Privacy Threshold Analysis. USDA APHIS, including the VS Management Team, is all responsible for protecting the privacy rights of the customers identified in the UFS as required by applicable State and Federal laws. Specific mitigation activities are:

- Appropriate database authentication is used to gain access to the system. User roles are established to ensure users have access to certain types of data based on their roles and need to access certain types of data in this system.
- User access is restricted within the system to relevant data. 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. A user may be restricted to the

information only pertaining to their particular state while others may have access to multiple sets of data.
- All organizational users are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training
- At the login screen of the application the warning banner must be acknowledged before users are allowed access.

2 Uses of the Information UFS

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 UFS automates the tracking, collection, and processing of fees due to Veterinary Services for its services provided at remote offices, import centers, port offices, or the National Veterinary Services Laboratories in Ames, Iowa.

The information collected on individuals is used to assess billing and collecting user fees for services provided by Veterinary Services, bill the customer for services rendered, and reconcile general ledger accounts at NFC.

Veterinary Services also uses the information on types of fees charged for import and export activity analysis; and the information on amounts charged and payments received are used in workload analysis at Area Offices and Land Border Ports.

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

Data is analyzed by running standard UFS reports using Oracle Reports. Authorized users can also run specific, customized queries and extract the data into spreadsheets for analysis.

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

UFS 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.

- Access to UFS is controlled by a database authentication solution.
- The application contains security measures to limit access to relevant information and prevents access to unauthorized information.
- At the login screen of the application the warning banner must be acknowledged before users are allowed access. .
- Security controls within the application are reviewed each year by independent assessors in order to verify that they are operating as expected.
- Access to personal information is restricted to individuals with a need to know in order to perform functions associated with their job.
- All organizational users are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training. Failure to comply with Rules of Behavior could result in strict disciplinary action, including termination or other adverse action that is deemed appropriate.

3 Retention UFS

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

3.1 How long is information retained?

Electronic data is maintained in the database and on the file server for 7 years. Archived data is maintained indefinitely in a table with read-only access. Paper records are maintained for 6 years, 3 months.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention period has been approved by NARA. The UFS records are scheduled under N1-463-10-002.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The data is monitored by the USDA UFS team. Because of the constant change and update of information, the data is continuously monitored by system users who regularly review the data by running reports and queries. This type of review and monitoring ensures the information in the system is accurate and up to date. Safeguards are in place to ensure that data is restricted to only authorized individuals. UFS maintains this information in a secure manner and disposes of information per APHIS Directive 3440.2.

4 Internal Sharing and Disclosure UFS

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

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

All data is available to the APHIS VS Offices for which they have responsibility.

APHIS MRPBS financial staffs, APHIS VS regional and national staff have access to the data for program implementation, oversight, and reporting.

Information in the UFS is transmitted to the USDA National Finance Center (NFC).

The only users with direct access to the system will be those internal to APHIS who have been granted access to the system. These will include System Administrators and Database Administrators, in addition to assigned APHIS personnel responsible for auditing and querying data in the application.

4.2 How is the information transmitted or disclosed?

The VS UFS users have access to the information system and can extract summary and detailed reports that are pertinent to their organizations.

The data that is pertinent to National Finance Center (NFC) is transmitted using secure File Transfer Protocol.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Unauthorized disclosure of personal information is the primary privacy risk to information shared internally to APHIS. These risks are mitigated through UFS, APHIS AEI GSS and NITC GSS security controls as delineated in the current UFS System Security Plan.

User access is restricted within the system to relevant data. 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. A user may be restricted to the information only pertaining to their particular state while others may have access to multiple sets of data.

5 External Sharing and Disclosure UFS

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?

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, records maintained in the system may be disclosed outside USDA as follows:

(1) To certain Federal agencies, including the Department of the Treasury, to obtain assistance in identifying and locating individuals who are delinquent in their payments of debt owed to the Federal Government while receiving Federal salary, tax refunds, or benefit payments, for the purpose of collecting debts;
(2) To a debt collection agency when USDA determines that such referral is appropriate for collecting the debtor's account as provided for in 31 U.S.C. 3718;
(3) To the appropriate agency, whether Federal, State, local, or foreign, charged with responsibility of investigating or prosecuting a violation of law or of enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a

violation or potential violation of law, whether civil, criminal, or regulatory in nature, and either arising by general statute or particular program statute, or by rule, regulation, or court order issued pursuant thereto;

(4) To the Department of Justice when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee or the United States, in litigation, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which the records were collected;

(5) For use in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected;

(6) To appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, a risk of identity theft or fraud, or a risk of harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(7) To contractors and other parties engaged to assist in administering the program. Such contractors and other parties will be bound by the nondisclosure provisions of the Privacy Act. This routine use assists the agency in carrying out the program, and thus is compatible with the purpose for which the records are created and maintained;

(8) 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

(9) To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

Information in the UFS may be disclosed to a consumer reporting agency when USDA determines that such referral is appropriate in accordance with 31 U.S.C. 3711(f).

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Where the Department controls the personally identifiable information in the UFS; use of that information will be governed by an appropriate routine use in SOR Notice, APHIS 1. APHIS VS works with State authorities on data protection through written agreements, such as Memoranda of Understanding, Interconnectivity Agreements, and Cooperative Agreements.

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

Information is shared through role-based access within the application and to reports generated by the application processes.

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

Unauthorized disclosure of personal information is the primary privacy risk to information shared internally to APHIS. These risks are mitigated through UFS, AEI & NITC GSS security controls through general and privileged access control policies, including required

authentication and authorization; annual user access reviews; and audit monitoring and review.

6 Notice UFS

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.

USF SORN

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

A System of Record Notice has been published in the Federal Register for the User Fee System under SORN APHIS-18.

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

In part, yes. Customers may decline to provide social security number or taxpayer identification number by choosing not to pay user fees with an APHIS credit account. However, all customers must provide basic contact information, such as name and address, in order to maintain program records and have contact information in case of an under- or over-payment.

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. All the data is treated uniformly from all customers. Once the data is gathered it is subject to all routine uses.

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.

Notice is provided on the APHIS Form 192 and by way of the published System of Record Notice. No information is collected without an individual's awareness.

7 Access, Redress and Correction UFS

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

7.1 What are the procedures that allow individuals to gain access to their information?

Any individual may obtain information from a record in the system that pertains to him or her. Requests for hard copies of records should be in writing, and the request must contain the requesting individual's name, address, name of the system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

Customers can contact the APHIS Office where the APHIS 81 was issued and request correction of inaccurate or erroneous information. The VS field office makes the corrections if deemed correct, and re-transmits the data to the National UFS database.

Any data the is collected or maintained under the Privacy Act should be corrected 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?

Customers are issued a hardcopy APHIS 81 with a phone number and instructions to contact the APHIS Office that provided the service if they have questions.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

The primary risk associated with the redress process is the loss of the written request. If the written request is mailed, the U.S. Post Office handling practices are the primary mitigations to data loss. Hand carried requests by the requester are the requesters responsibility to protect. Once received by the VS the requests are treated as sensitive material in accordance with the formal redress methods. Non-APHIS persons do not have access to UFS, so individuals cannot login to the system and correct their own information. In accurate personal information must be corrected by users at the time of business transactions or after by following redress procedures in 7.2 or 7.4.

8 Technical Access and Security UFS

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 UFS 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 UFS information are further controlled through electronic role-based access. Users must have a government issued login and password that is controlled and managed either at the Veterinary Services Regional or Area offices. Password controls, procedures, responsibilities and policies follow USDA departmental standards. Further annual review of user access is perform to ensure that appropriate access is given to the right individuals and to remove access when it is no longer needed.

8.2 Will Department contractors have access to the system?

VS IT contractors are provided access only as needed to perform the requirements of a given contract. Privacy clauses are included in the associated contracts and all contractors must complete a background checks per Department Human Resource policies. Contractors will not be involved in the production support of the application.

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 the UFS 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. This general training allows organizational users with access to personally identifiable information to receive privacy-related training.

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

The UFS received an Authority to Operate in June 2014.

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

Formal auditing measures for the UFS will include security assessments performed by 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 UFS Re-certification.

As to technical safeguards:

- The UFS is continuously monitored in several different ways. AEI GSS and NITC perform a monthly scan of systems to identify possible threats. The vulnerabilities identified are required to be remediated by the responsible parties. Security related incidents are reported to the ISSM which in turn requires an investigation. Also, all computers located within APHIS are required to have USDA-approved antivirus software installed. Once installed, the configuration is setup to receive updates twice weekly and to scan the machine daily. In addition, APHIS Customer Service Representatives have configured Windows Update to run on all machines for which they are responsible.
- The AEI GSS and NITC scan all systems at least every thirty days. This is conducted through the NITC/VS Reimbursable Agreement and results provided to the VS Program Support Services staff.
- Operational technical safeguards to prevent data misuse begin with access control. UFS employs SSL encryption to protect data during transmission. Access to UFS information is protected by role-based access which is managed by the network firewall and the UFS application. Users must have a government issued login and password that is controlled and managed either at the Veterinary Services. Password controls, procedures, responsibilities and policies follow USDA departmental standards. UFS users are APHIS employees and therefore, must use LincPass to access their computer and the APHIS network, including the VPN. At most sites, responsibility and scope of data access is defined by users' job descriptions. Policy dictates that a user may 'self-nominate' themselves for access. Requests for access must be approved by a supervisor or APHIS authorizing official.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what

privacy risks were identified and how do the security controls mitigate them?

Unauthorized disclosure of employee and other personnel information is the primary privacy risk to information shared within the USDA. This risk is mitigated through technical and procedural information security controls levied on internal holders of

UFS data. UFS and NITC GSS technical security controls are delineated in the current UFS System Security Plan.

9 Technology UFS

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?

Unauthorized disclosure of employee and other personnel information is the primary privacy risk to information shared within the USDA. This risk is mitigated through technical and procedural information security controls levied on internal holders of UFS data. UFS and NITC GSS technical security controls are delineated in the current UFS System Security Plan.

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

The UFS application does not employ technology that may raise privacy concerns.

10 Third Party Websites/Applications UFS

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. OMB M-10-23 has been distributed by APHIS VS.

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

UFS does not use 3rd party websites and/or applications.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

UFS does not use 3rd party websites and/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?

UFS does not use 3rd party websites and/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?

UFS does not use 3rd party websites and/or applications.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

UFS does not use 3rd party websites and/or applications.

If so, is it done automatically?

UFS does not use 3rd party websites and/or applications.

If so, is it done on a recurring basis?

No PII is made available. These products are used to validate existing information.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

UFS does not use 3rd party websites and/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?

UFS does not use 3rd party websites and/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)?

UFS does not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

UFS does not use 3rd party websites and/or applications.

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

UFS does not use 3rd party websites and/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?

UFS does not use 3rd party websites and/or applications.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

UFS does not use 3rd party websites and/or applications.

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.

UFS does not use 3rd party websites and/or applications.

ABSTRACT-Veterinary Services Laboratory Submissions (VSLS)

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format: ·

- This Privacy Impact Assessment (PIA) is for the USDA, APHIS, Veterinary Services (VS), Veterinary Services Laboratory Submissions (VSLS) system.
- VSLS is an enterprise-level (business-wide) electronic information management system. It will provide an electronic means of data input, data transmission, data storage, and data reporting. This system will enable 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 because the system collects personally identifiable information.

OVERVIEW-VSLS

VSLS is owned by USDA APHIS Veterinary Services and supports the staging of lab submission data for surveillance program systems such as SCS. It includes modules for CSF, BSE, Scrapie and Wildlife Services AI. Additionally it hosts a module for the California Avian Health Group.

VSLS is a “Major Application” with a FIPS-199 classification of “Moderate”.

1 Characterization of the Information VSLS

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?

The information in the VSLS may contain the following information types: Name, address, contact telephone, e-mail address for collectors, submitters and herd/flock owners, or associated APHIS personnel (Scrapie Epidemiologist), latitude/longitude coordinates, operation type(s), species and breeds, national premise identification number or other location identifier, flock or herd identification numbers, characteristics of the animal or specimen collected, testing an test results. VSLS can also be used to monitor the dates and times between sample collection and results entry, and the database maintains an audit of the users that created and/or updated collection information or results in the underlying database.

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

Information in this system is entered by state, federal and federally contracted personnel.

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

The purpose of the VSLS is to stage laboratory testing results before submitting them to the appropriate production system. In this way, an attempt is made to ensure that the collection site information and the testing and test results have been recorded with accuracy and integrity. This information is collected because it is important to animal health surveillance on non-FAD (Foreign Animal Disease) conditions.

Sharing of this information is handled by other VS IT systems, which will be referred to as destination systems. The VSLS itself is not a repository of record for the complete data, since it is used only for the aforementioned purpose of staging lab submissions. VSLS uses Jasper reports that look at the data in WDB underlying database tables and, in some cases, the destination VS system to ensure successful staging and loading of the data.

1.4 How is the information collected?

Collection site information including premises address and contact information, flock/herd owner and samples collected are entered by Federal employees or federally contracted

employees, the latter especially at slaughter markets. Test results are entered generally by state personnel working in one of the NAHLN laboratories around the country.

All are users of the system and must have eAuthentication level 2 credentials.

1.5 How will the information be checked for accuracy?

Program management staff, laboratory personnel, and in the case of non-negative test results, staff at the VS National Veterinary Service Laboratory (NVSL) all review and check the data for accuracy. Additionally, completeness of the information is validated on entry so that required fields are not left blank.

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

- 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 Stat674-678

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

- 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 VSLS system.
- All access to the system is controlled by USDA eAuthentication system or username and password.
- APHIS employees must authenticate with HSPD12 before connecting to the network.
- Application limits access to relevant information and prevents access to unauthorized information. Including enforcing state privacy using row level security in the underlying Oracle repository.
- All users receive formal system training and are required sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training
- At the login screen of the application the warning banner must be acknowledged before users are allowed access

2 Uses of the Information VSLS

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

In exceptional reporting support cases, such as for the current Scrapie SCS system, APHIS surveillance business analysts have been allowed to produce reports against the VSLS database directly using their Business Intelligence (BI) tools, until reporting can be developed against the management repository.

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

Data can be examined using the Jasper reports in VSLS that support extraction to excel or pdf. Business Intelligence and Analysis tools such as SAS and Alteryx may also be used (in exceptional circumstances –see 2.1) against the underlying database directly.

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

The system passes latitude and longitude to the USGS Watershed web services. These services return the Hydrologic Unit Code (HUC) in which the latitude and longitude lie, if it can be found, otherwise nothing is returned.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

- Privacy rights of the customer and employees will be protected by USDA APHIS VS management. VSLS 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 supervisormust identify (authorize)what functional roles that individual needs in the VSLS application.

- All access to the system requires user identification andauthentication with eAuth Level 2 credentials, and HSPD12 credentials for APHIS employees.
- The application limits accessto authorized information and prevents access to unauthorized information. In particular, state privacy is enforced in the underlying database through row level security in the physical data repository; this cannot be compromised by the VSLS web application component as it is not controlled by the web application.
- Detailed reportswith personal information will be labelled with the appropriate sensitive markings.
- All organizational users receive formal systemtraining and are required to sign rules of behavior before being given access to the system.
- At the login screen of the application thewarning banner must be acknowledged before users are allowed access.

3 Retention VSLS

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

3.1 How long is information retained?

VSLS data is retained in the production system for two years. Records older than two years are placed in a read only access tables and is not viewable with the VSLS application.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

No. The APHIS Electronic Records Scheduling Request (MRP 400) is in progress.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The data are maintained in accordance with APHIS records retention schedules that are applicable to the system. Note that submission forms contain data of limited use. Personally Identifiable Information **(**PII**)** is limited to names, addresses, and email and phone numbers of submitters, collectors or herd/flock owners. VSLS will

maintain the information in a secure manner such as access control procedures, and dispose of it only in conformance with an approved disposition authority from NARA.

4 Internal Sharing and Disclosure VSLS

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?

VS Surveillance program staff and management; VS NVSL staff and management; VS surveillance business analysts (in exceptional circumstances) and Wildlife Services staff and management have access to the data.

Please note that VSLS ‘shares’ data by sending it to the relevant VS systems using a combination of VS Rhapsody processing and PL/SQL database scripts. It is from those internal systems that the data may be further shared with relevant business stakeholders.

4.2 How is the information transmitted or disclosed?

VS Rhapsody and PL/SQL database scripts.

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.

Privacy risks, in general, are borne by the destination VS system as the data loading to those systems is automated and internal. There is a risk that a surveillance analyst who is granted direct access to the database for stopgap reporting might disclose information. However, these individuals are APHIS employees and must complete annual security awareness training and sign Rules of Behavior. They are only granted read only access to the data access and is approved by APHIS 513 access authorization form.

5 External Sharing and Disclosure VSLS

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?

VSLS is not intended for information sharing with external organizations. Such sharing is accomplished through the systems that use the data VSLS provides them. However, data may be shared with a few select state and federal agencies.

Federal and State animal health officials use the information to monitor the status of an animal disease investigation, document actions taken relating to an animal disease investigation, track the status of animals susceptible to foreign animal diseases, and assist with managing and analyzing animal disease and surveillance programs.

Federal and State wildlife agencies use the information to assist in managing and analyzing disease programs and monitoring diseases related to wildlife, feral or alternative livestock.

Department of Justice may use the information when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, in litigation, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the

information contained in the records that is compatible with the purpose for which the records were collected.

For use in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee, or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected;

To appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, a risk of identity theft or fraud, or a risk of harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and the disclosuremade to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

To contractors and other parties engaged to assist in administering the program. Such contractors and other parties will be bound by the nondisclosure provisions of the Privacy Act. This routine use assists the agency in carrying out the program, and thus is compatible with the purpose for which the records are created and maintained;

To USDA contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends or anomalies indicative of fraud, waste, or abuse; and

To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please

describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

VSLS is covered under the umbrella of the AHSM SORN (APHIS-15).

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

Please see previous section; information is not shared directly, but the California Animal Health Group Pilot Project users have access to the Jasper Reports in VSLS which are used to monitor work in progress. These reports can be downloaded in excel or PDF format.

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

The privacy risks are that the data may be used in a way not intended by VSLS when it was collected, and not documented in the published System of Records of Notice.

6 Notice VSLS

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

The data in the VSLS are covered by the following SORNs.

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

The published System of Record Notice (SORN) is the notice to the public.

6.3 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

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. The data are treated uniformly for all submitters. Once the information is submitted it is subject to all routine uses.

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

The System of Record Notice is the official notice. The uses of the data is outlined in this notice. No information is collected without an individual's awareness. At the time of data collection, a form is being completed or the individual is speaking with a Federal or State employee.

Information pertains to health status and location of an individual's animals

7 Access, Redress and Correction VSLS

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Any individual may obtain information from a record in the system that pertains to him or her. Requests for hard copies of records should be in writing, and the request must contain the

requesting individual's name, address, name of the system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

Inaccurate data are corrected by submitting requests to USDA APHIS Veterinary Services employees, state employees and or other federal employees and approval of the program manager is required in order for corrections to be made.

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

Individuals are notified of procedures by the animal health officials at the point of data collection.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

Any data used or furnished to others except as documented above would need to be cleared through the Freedom of Information Act process. Data are all submitted voluntarily by customers who seek out government services from the USDA or as part of an animal disease

investigation. Other USDA agencies may supplement this data. Incorrect data are corrected only with high level authorization, and corrected data are furnished to individuals affected.

8 Technical Access and Security VSLS

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 VSLS 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.

8.2 Will Department contractors have access to the system?

VS IT contractors are provided access only as needed to perform the requirements of a given contract, and only to test and development systems.

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 VSLS 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.

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

The VSLS completed Assessment and Authorization and received Authority to Operate in June 2014.

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

Auditing is enabled within the application for defined auditable events including modification to VSLS schema objects and unsuccessful and/or unauthorized access attempts. Tables have create and update time stamps and the user is captured. Important tables also have an

associated journal table that tracks all changes made. Audit monitoring, analysis and reporting are implemented according to internal Standard Operating Procedures.

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?

There is a risk that personal information collected on individuals (may be distributed beyond the intended audiences. VSLS has access controls in place to ensure that only individuals with a valid need-to-know/need-to-share have access to the information in the database. Also, VSLS reports are marked with appropriate sensitivity labels.

9 Technology VSLS

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 VSLS is a staging application that joins collection site information with testing results on the samples submitted from the collection site. It is in the operational and maintenance phase of its life cycle. It is designed to enhance the integrity of the destination VS system it serves by allowing lab submissions to be staged and reviewed before loading the information to the systems.

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.

10 Third Party Websites/Applications VSLS

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. 0MBM-10-23 has beendistributed by APHISVS.

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

The USGS web services are used to get the HUC associated with a latitude/longitude pair and the call to those services does not send any other information. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

10.3 What personally identifiable information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

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. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

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. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not applicable. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

If so, is it done automatically?

Not applicable. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

If so, is it done on a recurring basis?

Not applicable. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

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. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

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. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

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. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

10.10 Does the system use web measurement and customization technology?

Not applicable. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context.

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

Not applicable. This information transaction does not involve any PII data, it is strictly a geographical information exchange with no context. .

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.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

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.

This application does not employ technology which may raise privacy concerns.

ABSTRACT-Veterinary Services Process Streamlining (VSPS)

- This Privacy Impact Assessment (PIA) is for the USDA, APHIS, Veterinary Services (VS), Veterinary Services Process Streamlining (VSPS).
- VSPS is an enterprise-level (business-wide) information system that collects and stores data entered by importers for import permit requests and accredited veterinarians for accreditation applications, export health certificates, and interstate movement health certificates.
- This PIA was conducted as part of APHIS continuous monitoring activities.

OVERVIEW-VSPS

The Veterinary Services Process Streamlining (VSPS) system is classified as a major application by USDA/APHIS/VS. VSPS was developed using a Rapid Application Development approach with phased releases of modules and functionality. Modules were rolled-out for user testing and acceptance as they are completed. The following provides the status and timeframes for each module that is currently within the scope of the VSPS project.

VSPS currently consists of six major subsystems. The core component provides user maintenance and system administration functions. The other five components represent the mission areas that contain the primary functions required to capture the information needed to track animal and animal product movement into, out of, and within the United States. Each mission area component includes forms that must be automated into a cohesive system so that information can be captured in a timely and accurate manner.

VSPS uses Mobile Information Management (MIM) technology to capture data in the field. This technology allows the user to capture the data in field with a personal desktop assistant, and then when back at the duty location, use the Desktop Management application to synchronize and upload the data to the VSPS database in Fort Collins, CO.

1 1 Characterization of the Information VSPS

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?

The VSPS system collects information from veterinarians (name, address, date of birth, phone number) who apply on-line to become federally accredited, from importers that are requesting a permit to import animals, and from accredited veterinarians that are submitting health certificates for the export and interstate movement of animals.

VS personnel processes and approve applications for federal accreditation, document actions taken against accredited veterinarians, process permit requests and issue import permits,

maintain the animal import rules, process export health certificates, and maintain the export protocols. State personnel issue permits for interstate movement requests and maintain the state protocols.

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

The primary sources of information collected and stored in the VSPS system are data entered by importers for import permit requests and accredited veterinarians for accreditation applications, export health certificates, and interstate movement health certificates.

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

- **Veterinary Accreditation:** VS relies upon accredited veterinarians to attest to the health of animals at the time of inspection being exported to foreign countries or being moved between or within States. A veterinarian must be accredited in each state in which he or she performs Federal work. The Veterinary Accreditation module automates submission of the accreditation application; streamline the approval process through the electronic distribution of information, and record actions taken against accredited veterinarians.
- **Live Animal Import:** All animals entering the United States must go through an Import Process. The Animal Import module will capture data real time of animals entering the United States through all of its ports including land border ports, animal import centers, limited ports and Ocean and Air ports. This module also supports on-line processing for the arrival and release of animals entering the United States.

- **Interstate Animal Movement**: All animals being moved from State to State are required to go through an Interstate Movement Certification Process. Each animal must be inspected by an accredited veterinarian and will be subject to the target State's entry regulations. The Interstate Animal Movement module automates the way accredited veterinarians process animal health information, including laboratory test results and processing of the final health certificate required for entry into the target State. This module also provides a mechanism for capturing permits by the State for requested interstate movements.
- **Facilities:** allows current National Import Export Services (NIES) animal import product staff to enter information about facilities that receive and treat animal import products from a number of countries around the world.

Another aspect of this module is a Facility Approved to Export Animal Products (FAEAP). These are facilities that are authorized or approved to export certain animal products to specific countries or geographic regions. Approval is dependent upon criteria established by the importing country or region. Criteria may vary depending on the approved activity. The criteria for approval and details related to an approval may change frequently.

1.4 How is the information collected?

The information is collected through user data input as well as uploaded via a Mobile Information Management device through an encrypted process.

1.5 How will the information be checked for accuracy?

All data collected and stored in the VSPS system is provided by either a customer (importer, State Regulatory Official (SRO), and Accredited Veterinarian) or VS personnel.

The data associated with an accredited veterinarian is maintained by the customer (user) that provided the original information. These users have fully access to the data that pertains to them, so the accuracy of the data is controlled by the customer and owner of the data. In addition, these users will be prompted by the VSPS system to verify and update their data every 6 months to ensure the data remains current and accurate.

The data associated with imports, exports, interstate movement, and slaughter horse transport are transactional in nature. Once a request is processed to completion, which should take no longer than 90 days, the data is retained as read only and will not be changed. The timeliness, accuracy, and completeness of this data will not be an issue.

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
- 21 U.S.C. 105, 111-114a-1, 116, 125, 134b, 134f
- Title 9, Code of Federal Regulations (9 CFR)

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 customer personally identifiable data is the primary privacy risk as identified in the PTA. USDA APHIS, including the VSManagement Team, District Directors, Veterinary Medical Officers (VMO), National Import Export Services program staff and State Regulatory Officials are all responsible for protecting the privacy rights of the users identified in VSPS. Specific mitigation activities are:

- All access to the data in the system is controlled by an authorization process. An APHIS point of contact or supervisor must identify (authorize) what functional roles that individual needs in the VSPS system.
- All access to VSPS is controlled by the USDA eAuthentication system.
- The application limits access to relevant information and prevents access to unauthorized information.
- All organizational users are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training
- At the login screen of the application the warning banner must be acknowledged before users are allowed access.

2 Uses of the Information VSPS

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

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

The IBM Cognos Enterprise business intelligence tool is used to analyze the data collected in VSPS.

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

VSPS uses Google Maps to identify directions to a specific address for the interstate movement of animals.

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.

- All access to VSPS is controlled by the USDA eAuthentication system.
- The application contains security measures to limit access to relevant information and prevents access to unauthorized information.
- At the login screen of the application the warning banner must be acknowledged before users are allowed access.
- Security controls within the application are reviewed each year by independent assessors in order to verify that they are operating as expected.
- Access to personal information is restricted to individuals with a need to know in order to perform functions associated with their job.
- All organizational users are required to sign Rules of Behavior on an annual basis as part of the USDA mandatory information system security awareness training. Failure to comply with Rules of Behavior could result in strict disciplinary action, including termination or other adverse action that is deemed appropriate.

3 Retention VSPS

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

3.1 How long is information retained?

APHIS maintains information about accredited veterinarians in the system indefinitely. This includes veterinarians whose accreditation has lapsed or been revoked. However, APHIS destroys only the paper files when a veterinarian is deceased. The system also contains information about veterinarians who are applicants for accredited status.

The retention period for data associated with the import of animals, export of animals, interstate movement, and slaughter horse transport is planned to be 7 years.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

This is in progress. VSPS is taking necessary action to ensure that the MRP 400 is completed and submitted to NARA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Unauthorized disclosure of employee and other personal data is the primary privacy risk, as identified by the PTA. To mitigate this risk data is maintained and disposed of in accordance with APHIS records retention schedules that are applicable to the system. Safeguards are in place to ensure that data is restricted to only authorized individuals. Personally Identifiable Information (PII) is limited to name, mailing address, phone number, State license number, and score on accreditation examination. VSPS maintains this information in a secure manner.

4 Internal Sharing and Disclosure VSPS

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?

Not applicable. The information within VSPS is not shared internally.

4.2 How is the information transmitted or disclosed?

Not applicable.

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.

Not applicable.

5 External Sharing and Disclosure VSPS

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?

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, records maintained in the system may be disclosed outside USDA as follows:

(1) To State animal health officials in each State, State veterinary examining or licensing boards, and the American Association of Veterinary State Boards to certify accreditation or license status or exchange information regarding disciplinary action(s);
(2) To the public for the purpose of locating and contacting accredited veterinarians in a specific geographical area;
(3) To the appropriate agency, whether Federal, State, local, or foreign, charged with responsibility of investigating or prosecuting a violation of law or of enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and either arising by general statute or particular program statute, or by rule, regulation, or court order issued pursuant thereto;
(4) To the Department of Justice when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, in litigation, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which the records were collected;
(5) For use in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee, or the United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation,

and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected;

(6) To appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, a risk of identity theft or fraud, or a risk of harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

(7) To contractors and other parties engaged to assist in administering the program. Such contractors and other parties will be bound by the nondisclosure provisions of the Privacy Act. This routine use assists the agency in carrying out the program, and thus is compatible with the purpose for which the records are created and maintained;

(8) To USDA contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends or anomalies indicative of fraud, waste, or abuse;

(9) To a congressional office from the record of an individual in response to an inquiry from the congressional office made at the written request of that individual; and

(10) To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Where the USDA controls the personally identifiable information in the VSPS application; use of that information will be governed by an appropriate routine use in a SOR Notice APHIS-2. Where the VSPS information is controlled by State authorities, the legal mechanisms employed are per state information security law and regulation. APHIS VS

works with State authorities on data protection through the use of NDAs, ISAs, MOUs and other agreements.

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

Current information is shared through role-based access to the VSPS Cognos reports, as well as through role-based access within the application.

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

Unauthorized disclosure of personal information is the primary privacy risk to information shared internally to APHIS. Before data is shared externally, a review of the VSPS System of Record Notice (SORN) is performed to ensure that the sharing is documented as a Routine Use, and also that the sharing is compatible with the mission and purpose of the VSPS. These risks are mitigated through VSPS and NITC GSS security controls as delineated in the current VSPS System SecurityPlan.

6 Notice VSPS

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.

VSPS SORN

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

Information is collected on an OMB approved APHIS forms, which contain Privacy Act Statements.

A System of Record Notice has been published in the Federal Register for the Records of Accredited Veterinarians under USDA-APHIS-2.

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

No, if information is required the user must provide that information or, not use the VSPS application.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The data are treated uniformly for all submitters. Once the information is submitted it is subject to all routine uses.

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

The System of Record Notice is the official notice. No information is collected without an individual's awareness. At the time of data collection, a form is being completed or the individual is speaking with a Federal or State employee.

7 Access, Redress and Correction VSPS

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

7.1 What are the procedures that allow individuals to gain access to their information?

Any individual may obtain information from a record in the system that pertains to him or her. Requests for hard copies of records should be in writing, and the request must contain the requesting individual's name, address, name of the system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700River Road Unit 50, Riverdale, MD 20737-1232.

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

Users can directly correct any inaccurate or erroneous information that pertains to them by accessing their User Profile in VSPS. A user may also contact the VSHelp Desk for assistance in correcting inaccurate or erroneous information. Help Desk personnel will investigate and notify VSPS Program staff to verify the request. If after investigation, the data is found to be inaccurate or the data can no longer be verified, the data will be corrected.

Any data the is collected or maintained under the Privacy Act should be corrected 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?

Notification is provided at the time a user is creating their VSPS User Profile.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

The primary risk associated with the redress process is that the request will be ignored or delayed by the VSPS Program or IT staff. If the written request is delivered to the address as stated in Section 7.4, and then requested by the APHIS Privacy Office, VS is mandated to comply with Privacy requirements. VS makes every attempt to act on requests by conducting rapid reviews of the request, and coordinating a response with the Privacy Office to ensure that requested timeframes are met.

8 Technical Access and Security VSPS

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 VSPS 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 VSPS information are further controlled through electronic role-based access. Users must have a government issued login and password that is controlled and managed either at the Veterinary Services Regional or District Offices.HSPD-12 LincPass cards, procedures, responsibilities and policies follow USDA departmental standards.

8.2 Will Department contractors have access to the system?

VS IT contractors are provided access only as needed to perform the requirements of a given contract. Contractors are involved in the design and development of the VSPS. Privacy clauses are included in the associated contracts. Contractors will not be involved in the production support of the application.

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 the VSPS application are required to complete annual Information Technology (IT) Security Awareness Training andmust sign APHIS Rules of Behavior form prior to receiving access to the information system.

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

The VSPS has completed Assessment and Authorization and received its Authority to Operate in June 2014.

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

Formal auditing measures for the VSPS will include security assessments performed by APHIS at least annually and independent security assessments performed in support of Certification and Accreditation efforts.

As to technical safeguards:

- The VSPS is continuously monitored in several different ways. NITC perform a monthly scan of systems to identify possible threats. The vulnerabilities identified are required to be remediated by the responsible parties. Security related incidents are reported to the ISSM which in turn requires an investigation. Also, all computers located within APHIS are required to have USDA-approved antivirus software installed. Once installed, the configuration is setup to receive updates twice weekly and to scan the machine daily. In addition, APHIS Customer Service Representatives have configured Windows Update to run on all machines for which they are responsible.
- NITC scans all systems at least every thirty days. This is conducted through the NITC/VS Reimbursable Agreement and results provided to the VS Program Support Services staff.
- Operational technical safeguards to prevent data misuse begin with access control. VSPS employs SSL encryption to protect data during transmission. Access to VSPS information is protected by role-based access which is managed by the network firewall, eAuthentication, and the VSPS application. Users must have a government issued login and password that is controlled and managed either at the Veterinary Services or Area offices. Password controls, procedures, responsibilities and policies follow USDA departmental standards. At most sites, responsibility and scope of data access is defined by users' job descriptions. Policy dictates that a user may 'self-nominate' themselves for access. Requests for access must be approved by a supervisor or APHIS authorizing official.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Unauthorized disclosure of employee and other personnel information is the primary privacy risk to information shared both internally and externally to the USDA. This risk is mitigated through technical and procedural information security controls levied on internal and external holders of VSPS data. VSPS and NITC GSS technical security controls are delineated in the current VSPS System Security Plan.

9 Technology VSPS

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 VSPS is an operational major application (MA). The data is used to support Veterinary Accreditation, Import of Animals, Export of Animals, Interstate Movement of Animals, and Slaughter Horse Transport, all of which are covered under Title 9, Code of Federal Regulations (9 CFR) Animals and Animal Products. The data collected within VSPS is also used for research, investigative and litigation support, comparative and risk analysis.

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

The VSPS application does not employ technology that may raise privacy concerns.

10 Third Party Websites/Applications VSPS

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. OMB M-10-22 and OMB M-23 have been distributed by APHIS VS.

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

Google Maps are currently used by Accredited Veterinarians to identify directions to a location of an animal. This is so the Veterinarian can examine the animal for interstate movement approval. The VSPS application re-directs users to the Google Maps website.

Pay.gov is also a third party application that is used to allow import brokers to pay for reservations at the Veterinary Services Animal Import Centers located inMiami, Florida and Newburg, New York. The VSPS application re-directs users to the Pay.gov website.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

VSPS does not receive any personally identifiable information from 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?

VSPS does not receive any personally identifiable information from 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?

VSPS does not receive any personally identifiable information from 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?

VSPS does not receive any personally identifiable information from third party websites or applications.

If so, is it done automatically?

VSPS does not receive any personally identifiable information from third party websites or applications.

If so, is it done on a recurring basis?

VSPS does not receive any personally identifiable information from 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?

VSPS does not receive any personally identifiable information from 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?

VSPS does not receive any personally identifiable information from 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)?

VSPS does not receive any personally identifiable information from third party websites or applications.

10.10 Does the system use web measurement and customization technology?

VSPS does not use web measurement or customization technology.

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

VSPS does not use web measurement or customization technology.

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?

VSPS does not use web measurement or customization technology.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

VSPS does not use web measurement or customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

VSPS does not use web measurement or customization technology.