

# Privacy Impact Assessment Template

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: May 21, 2015
- Prepared for: USDA OCIO-Policy,  
E-Government and Fair Information  
Practices (PE&F)





# **Privacy Impact Assessment for the VS NITC System (VNS): Veterinary Services Process Streamlining (VSPS)**

April, 2020

## **Contact Point**

**Orlando Baca**  
**USDA APHIS Veterinary Services**  
*(301) 851-3408*

## **Reviewing Official**

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

## Abstract

- This Privacy Impact Assessment (PIA) is for the USDA, APHIS, Veterinary Services (VS), Veterinary Services Process Streamlining (VSPTS).
- VSPTS 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

The Veterinary Services Process Streamlining (VSPTS) system is classified as a major application by USDA/APHIS/VS. VSPTS 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 VSPTS project.

VSPTS 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.

VSPTS 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 VSPTS database in Fort Collins, CO.

## Section 1.0 Characterization of the Information

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

### **1.1 What information is collected, used, disseminated, or maintained in the system?**

The VSPTS system collects information from veterinarians that 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 VS 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 VS Management 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.

## Section 2.0 Uses of the Information

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

### **2.1 Describe all the uses of information.**

The data 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 covered 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.

### Section 3.0 Retention

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

#### **3.1 How long is information retained?**

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)?**

The VSPS Records Scheduling Request was submitted to NARA for approval.

#### **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.

## Section 4.0 Internal Sharing and Disclosure

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

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

At this point, no other Federal or internal USDA agencies have been identified as requiring access to the data contained in VSPS.

### **4.2 How is the information transmitted or disclosed?**

The APHIS and state users have access to the VSPS through the Digital Infrastructure Services Center (DISC) General Support System (GSS) and can view detailed or summary reports that are pertinent to their organizations. User access to the information through login access to the application and access is controlled via application roles and location of the users.

### **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. Access controls are employed within VSPS to comply with least privilege requirements. Further, sharing risks are mitigated through VSPS and DISC GSS security controls as delineated in the current VSPS System Security Plan.

## Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

### **5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?**

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

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.**

Yes. The sharing of personally identifiable information outside the Department is compatible with the original collection. 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 DISC GSS security controls as delineated in the current VSPS System Security Plan.

## Section 6.0 Notice

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

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

VSPS SORN

[https://www.ocio.usda.gov/sites/default/files/APHIS\\_2\\_Tuesday\\_May\\_12\\_2015.txt](https://www.ocio.usda.gov/sites/default/files/APHIS_2_Tuesday_May_12_2015.txt)

**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.

## Section 7.0 Access, Redress and Correction

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

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

Any individual may obtain information from a record in the system that pertains to him or her. 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?**

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 VS Help 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 that 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.

## Section 8.0 Technical Access and Security

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

**8.1 What procedures are in place to determine which users may access the system and are they documented?**

Access to the 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 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 VSPS has completed Assessment and Authorization and received its Authority to Operate in June 2017.

### **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. DISC 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.
- DISC scans all systems at least every thirty days. This is conducted through the DISC/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 DISC GSS technical security controls are delineated in the current VSPS System Security Plan.

## Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

**9.1 What type of project is the program or system?**

The 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.

## Section 10.0 Third Party Websites/Applications

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

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

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

**10.2 What is the specific purpose of the agency’s use of 3<sup>rd</sup> 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 in Miami, 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> party websites and/or applications, discuss the privacy risks identified and how they were mitigated.**

VSPS does not use web measurement or customization technology.

## Responsible Officials

*Renee Oleck, APHIS Veterinary Services*  
United States Department of Agriculture



## Approval Signature

---

Orlando R. Baca  
VSPS System Owner  
United States Department of Agriculture

---

Preston Griffin  
APHIS CISO (Acting) & ISSPM  
United States Department of Agriculture

---

Tonya Woods  
APHIS Privacy Act Officer  
United States Department of Agriculture