

# Privacy Impact Assessment Animal Disease Traceability Information System (ADTIS)

Technology, Planning, Architecture, & E-Government

- Version: 1.4
- Date: June 4, 2012
- Prepared for: USDA OCIO TPA&E



# Privacy Impact Assessment for the Animal Disease Traceability Information System (ADTIS)

June 4, 2012

**Contact Point**

**Elinor Galleli**

**Animal and Plant Health Inspection Services (APHIS)  
Veterinary Services  
United States Department of Agriculture  
(970) 494-7333**

**Reviewing Official**

***Tonya Woods***

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

***Danna Mingo***

***APHIS Information Security Branch*  
United States Department of Agriculture  
(301) 851-2487**

## Abstract

- 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

The ADTIS contains four major components; Standardized Premises Information System (SPIS), Premises Allocator/ Repository, Animal Identification Management System (AIMS) and the Animal Tracing Processing System (ATPS). 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.

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.

- (3) 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.
- (4) Animal Tracing Processing System (ATPS) - is the application that would enable a single entry portal for animal health officials to request information to support disease traceback investigations. The ATPS is being allowed to lapse (2-2012) until more records are populated in internal and external information systems that the ATPS would communicate with.
- (5) The Animal Health Event Repository (AHER) is a data mart/warehouse repository that receives information from most of the other VS data stores and reports via a client back to the ATPS upon a request.

## 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?

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.

(5) 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.

## **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 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 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.

## **Section 3.0 Retention**

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

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

The 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 and disposes of information per APHIS Directive 3440.2.

## **Section 4.0 Internal Sharing and Disclosure**

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

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

USDA 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?**

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.

## 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 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.

## **Section 6.0 Notice**

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

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

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

**6.2 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.

**6.3 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.

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

The System of Record Notice is the official notice. 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.

## 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?**

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 ADTIS 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.

## 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 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 February 2014.

## 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. 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 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 Chief Information Office (CIO) Technology 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 CIO. 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.

## 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 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.

## 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”?

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 3<sup>rd</sup> party websites and/or applications?

Data from ZP4 or Tele Atlas, are used in ADTIS to validate premises addresses.



**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.**

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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> party websites and/or applications, discuss the privacy risks identified and how they were mitigated.**

ADTIS does not use web measurement or customization technology.

## Responsible Officials

Neil Hammerschmidt, Veterinary Services  
United States Department of Agriculture

Rajiv Sharma, (Acting) APHIS Information Systems Security Program Manager  
(ISSPM)  
United States Department of Agriculture

Marilyn Holland, APHIS Chief Information Officer  
United States Department of Agriculture

Tonya Woods, APHIS Privacy Officer  
United States Department of Agriculture

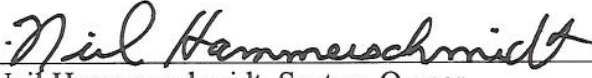
## Privacy Impact Assessment Authorization Memorandum


I have carefully assessed the Privacy Impact Assessment for the

\_\_\_\_\_  
(Animal Disease Traceability Information System (ADTIS))

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.


We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

  
\_\_\_\_\_  
Neil Hammerschmidt, System Owner

  
\_\_\_\_\_  
John Picanso, VS CIO

  
\_\_\_\_\_  
Dawn Tucker, Acting APHIS CIO

  
\_\_\_\_\_  
Rajiv Sharma, APHIS ISSPM

  
\_\_\_\_\_  
Tonya Woods, APHIS Privacy Officer

---