

Privacy Impact Assessment Generic Disease Database

Technology, Planning, Architecture, & E-Government

- Version: 1.2
- Date: January 3, 2012
- Prepared for: USDA OCIO TPA&E





Privacy Impact Assessment for the Generic Disease Database (GDB)

January 3, 2012

Contact Point

Elinor Gallelli

APHIS Veterinary Services

United States Department of Agriculture

(970) 494-7333

Reviewing Officials

Tonya Woods

Director, Freedom of Information and Privacy Act Staff

United States Department of Agriculture

(301) 734-8296

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), Generic Disease Database (GDB).
- The GDB is a legacy enterprise-level (business-wide) animal health and surveillance electronic information management system. The GDB is a central repository for APHIS VS and participating State animal disease/pest monitoring and management program information.
- This PIA was conducted because the GDB is undergoing security re-certification and collects personally identifiable information.

Overview

The Generic Disease Database (GDB) is an operational, legacy major application (MA) for which the USDA Animal and Plant Health Inspection Service (APHIS)/ Veterinary Services (VS) is responsible. The purpose of the GDB is to provide a national repository of animal disease and animal tracking information. The information contained in the GDB facilitates VS in its mission to protect and improve the health, quality, and marketability of the nation's animals, animal products, and veterinary biologics, and promote public health and environmental safety.

The GDB maintains test and/or vaccination data and other program information such as disease or certification status for flocks/herds subject to or involved with USDA APHIS VS animal disease/pest surveillance and or control programs such as: Johnes, Brucellosis, Tuberculosis, Chronic Wasting Disease, Pseudorabies, and Avian Influenza. Included in this functional data is privacy related data such as USDA and State employee name, address, and phone information for employees directly involved in the above mentioned program activities. The GDB supports the Veterinary Services mission to protect and improve the health, quality, and marketability of our nation's animals by providing a nationwide repository of animal health and productivity information.

GDB also maintains name, address, and phone information for individuals identified as contacts for premises (locations) and owners of animals or animal related operations involved with the various programs. Because of the variable nature of the premises, including sole proprietorships, and the undocumented relationship of the contact to the premises, many of the contacts are simply private citizens.

The GDB is funded by Congress through appropriated funds for the Animal Health Monitoring and Surveillance (AHMS) budget line item. The GDB has an Authority to Operate (ATO) letter dated 7/30/2008 and is security categorized as a "Moderate" system.

Section 1.0 Characterization of the Information

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

Information/Record Type	Component Data (Examples)
Premises	Physical location of a business or animal herd/flock.
Premises Supplemental Detail	Commercial operation records to provide additional details about the business, such as whether or not they are approved to receive international livestock.
Events	Events are activities such as tissue collections, vaccinations, inspections, or inventories.
Surveillance	Test results for diseases such as Johnes, Brucellosis, Tuberculosis, Chronic Wasting Disease, Pseudorabies, or Avian Influenza.
Other	Specific ad-hoc data.
Status	Temporary conditions or groups that a herd may be part of or subject to, such as quarantined, infected, certified free, or scheduled for future testing.
Aggregated	Instance of surveillance and program data that allows state-wide aggregation of data by species, disease, premises type, herd status and/or location (state, county, zip code).

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

- Employee – GDB maintains name, address, and phone information for USDA employees directly involved in disease program activities.
- Other -- GDB maintains name, address, and phone information for individuals identified as contacts for premises (locations) and owners of animals or animal related operations involved with the various animal disease/pest surveillance and or control programs. Because of the varying nature of the premises, including sole proprietorships, and the undocumented relationship of the contact to the premises, many of the contacts are simply private citizens deserving of protection under the Privacy Act.

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

There are three sources of information for the GDB, Federal, State/Local Government and third-party. The USDA Food Safety Inspection Service (FSIS), Farm Services Agency (FSA), APHIS (National Veterinary Services Laboratories (NVSL) and Wildlife Services), USDA National Agriculture Statistics Service (NASS) and US Post Office (address validation) currently provide data for use in the GDB application. The individual State Veterinarian Offices, as well as multiple state and private animal disease testing laboratories provide data for use in the GDB system.

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

The information is being collected to protect and improve the health, quality, and marketability of the nation's animals, animal products, veterinary biologics, and promote public health and environmental safety.

1.4 How is the information collected?

The information collected from states, users, individuals and/or businesses in the general public is collected on OMB approved- forms or directly as referenced in Information Collections numbers 0579-0047, 0579-0146, and 0579-0212. In some cases, the information is entered directly into the GDB application by animal lab employees who are entering results from their internal lab documents or a state or federal employee entering information provided over the phone, in an email, or letter by a producer typically in order to fulfill a request for a flock ID or ear tags.

1.5 How will the information be checked for accuracy?

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

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

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

1.6 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 Public Health Security and Bioterrorism Response Act of 2002
- 7 USC Sec. 7629

- The Farm Security and Rural Investment Act of 2002
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002 116 Stat 674-678
- The Homeland Security Presidential Directive 9.

Additional limitations are placed on the collection, use and dissemination of GDB information through the use of Memorandums of Understanding (MOUs) between the USDA APHIS VS and the local State APHIS offices inputting to local GDB instances.

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

Unauthorized disclosure of employee and other personal data, as identified in Section 1.1 above, was the primary privacy risk identified in the PTA. USDA APHIS, including the VS Management Team, Regional Directors, Area Veterinarian in Charge (AVIC), Centers for Epidemiology and Animal Health (CEAH), National Surveillance Unit (NSU) and State Veterinarians are all responsible for protecting the privacy rights of the customers and employees identified in the GDB as required by applicable State and Federal laws. Specific mitigation activities are:

- 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 GDB system.
- All access to the system is limited by username/password.
- Application limits access to relevant information and prevents access to unauthorized information.
- All users receive formal system training and 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 to log into the application

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The information contained in the GDB provides VS with an accurate and timely national animal health data that can be used to make decisions in emergency situations and respond to emerging issues, assess risks, and facilitate trade. Normally the data is used for routine animal health surveillance, management of domestic disease and pest control programs, and to monitor for and respond to the introduction of foreign animal diseases

- APHIS' Risk Analysis GIS group uses data from GDB to create mapping trends. When requested, GDB also supplies data to other Veterinary Services applications, including National Animal Disease Traceability System (ADTIS), Veterinary Services Process Streamlining (VSPS), Emergency Management Response System (EMRS), National Veterinary Services Laboratories (NVSL), Animal Health Surveillance and Management System (AHSM) and National Animal Health Laboratory Network (NAHLN).
- State Veterinarians and State Animal Health officials, as owners of the data, have the discretion to share data stored in the GDB in accordance with state laws and regulations via public web sites and/or may store such data in animal health surveillance databases developed by State IT developers, contractors or other third party software vendors in a manner that provides secure data access.
- The National Surveillance Unit (NSU) has agency responsibility for reporting surveillance activities on a nationwide basis. The NSU has direct access to the GDB and provides and publishes summarized data to the public and our trading partners. No 'customer', 'employee' or 'other' classifications of private data is published or distributed by NSU to external audiences.
- Certain disease information is reported by State and/or Federal animal health authorities. These reports are then summarized in reports to the (OIE) Office International des Epizooties (World Organization for Animal Health). No 'customer', 'employee' or 'other' classifications of private information is published or distributed to OIE.
- Selected animal disease data is shared with state and federal wildlife agencies, as animal diseases frequently crossover between domesticated animals and wildlife. All data, by definition, is shared with state animal health officials and state animal health databases.

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

Oracle based form and report aggregation tools are used for data correlation and/or extraction. Data is also analyzed in Excel spreadsheets and by using SAS a statistical application. Data is used to produce summary and detailed reports for stakeholders. Any other analysis is performed by tools outside of direct GDB control.

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

The GDB uses county codes that pre-populated in the database as a lookup field. These county codes are based on the US Post Office Federal Information Processing Standard (FIPS) county codes.

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.

- 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 GDB application.
- All access to the system requires user identification and authentication. Users must have a government issued login and password that is controlled and managed either at the Veterinary Services, National, Regional or Area offices or in the case of local State databases the State Veterinarian's office.
- The GDB application limits access to relevant information and prevents access to unauthorized information through role-based access control.
- Electronic access to GDB information is further protected by the AEI GSS network firewall, and network access control.
- All users receive formal USDA information system security awareness training and are required to sign rules of behavior before access to the application is granted. The GDB has additional security controls to address access/security of information.
- At the application login screen the warning banner must be acknowledged before users are allowed to log into the application.

Section 3.0 Retention

3.1 How long is information retained?

The records within the GDB application are considered permanent until the actual records retention scheduled is approved by NARA. Individual electronic records are retained within the system for 150 years minimum from the last date of creation, edit, or access of the individual records or their child records. The location of an animal disease infection is important to APHIS and TSE studies have shown that the disease agent may remain infectious in the environment for up to 16 years after outbreak and possibly longer.

Incremental and full system tape backups are retained for 1 month. APHIS ITD retains 1 full month backup for one year.

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. GDB 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, as identified in Section 1.1 above, is the primary privacy risk, as identified by the PTA. The benefit of having that data available for premises backtracking and other trending information during an emergency overrides any risk due to data retention timescale. To mitigate this risk data is maintained and disposed of in accordance with APHIS records retention schedules that are applicable to the system. Note that data entry forms contain data of limited use. Personally Identifiable Information (PII) is limited to names, addresses, email and phone numbers of submitters. GDB maintains information in a secure manner and disposes of information per APHIS Directive 3440.2.

Section 4.0 Internal Sharing and Disclosure

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

All data is available (for the Areas/states for which they have responsibility) to field (Area/state) personnel, regional and national staff for program implementation, oversight, and reporting.

National Center for Import Export gets summary data to assist in trade negotiations.

4.2 How is the information transmitted or disclosed?

VS users have access to the GDB through the APHIS Enterprise Infrastructure (AEI) General Support System (GSS) and can extract summary reports that are pertinent to their organizations.

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 employee and other personal information, as identified in Section 1.1 above, is the primary privacy risk to information shared internally to APHIS. The animal health professionals who analyze the data are trained in the proper use and dissemination of risk analysis data. From a technical perspective, a Plan of Action and Milestone (POA&M) #16479 was created in the Department's CSAM system to track the remediation of security controls associated with data sharing. The GDB system is being retired. The replacement application is

Surveillance Collaboration Services (SCS). As the GDB state users and their associated data are migrated to SCS, the ability to extract that same data from GDB is being removed.

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?

GDB information is shared with the following external organizations.

- GDB shares data with State cooperators and contractors, other Federal agencies (Health and Human Services, Center for Disease Control, and Department of Homeland Security). However, no direct access to the data in GDB is provided to these external organizations other than State cooperators. VS staff pulls data as needed.
- 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.
- Federal or State agencies involved with public health such as the Departments of Homeland Security and Health and Human Services use the information for the purposes of zoonotic disease surveillance or control activities.
- Other appropriate agencies, whether Federal, State, local, or foreign, use the information to assist 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.
- 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 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.
- 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.
- To USDA contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends or anomalies indicative of fraud, waste, or abuse.
- 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 GDB; use of that information will be governed by an appropriate routine use in a SOR Notice. Where the GDB 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 cooperative agreements.

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

State Animal Health users have access within the GDB to all data for the state in which they reside. This is compatible with the original collection and a SORN is in progress.

For any information sent in a report, the privacy information is redacted. When the external recipient is under contract with USDA Non-Disclosure Agreements are used to prevent unauthorized information transfer.

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

Unauthorized disclosure of employee and other personal information, as identified in Section 1.1 above, is the primary privacy risk to information shared externally to the USDA. This risk has been mitigated for USDA initiated sharing through technical and procedural information security controls levied on external holders and through the use of NDAs, ISAs, MOUs and other cooperative agreements.

The data access of state users is restricted to users within their state. From a technical perspective, a Plan of Action and Milestone (POA&M) #16479 was created in the Department's CSAM system to track the remediation of security controls associated with data sharing. The GDB system is being retired. The replacement application is Surveillance Collaboration Services (SCS). As the GDB state users and their associated data are migrated to SCS, the ability to extract that same data from GDB is being removed.

Section 6.0 Notice

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

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

A System of Record Notice has not been published in the Federal Register. However, this is in progress and is being tracked by a Plan of Action and Milestone in the USDA CSAM system under POA&M ID 13885.

The projected timeline for posting of the Notice in the Federal Register is November 28, 2011. Barring any re-writes due to comments from the public, this Notice should become active March 2012.

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

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

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

No. The data are treated uniformly for all submitters. Only information that is cleared through the Freedom of Information Act is available for other 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. 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. The information being collected is not of an extremely sensitive or personal nature. Information pertains to health status and location of an individual's animals.

Section 7.0 Access, Redress and Correction

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 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 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.

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

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

Access to the GDB 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 GDB 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 GDB. Privacy clauses are included in the associated contracts. Contractors will not be involved in the ongoing 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 individuals provided access to the GDB application are required to complete annual Information Technology (IT) Security Awareness Training and must sign an 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?

Certification and Accreditation was completed on 7/30/2008.

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

Initially, field data collection software uses a FIPS 140-2 certified encryption algorithm and data is removed from the collection device once it has been transmitted to GDB.

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

As to technical safeguards:

- The GDB is continuously monitored in several different ways. APHIS requires 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 Symantec Antivirus 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.
- APHIS scans all systems at least every thirty days. This is conducted by the APHIS Cyber Incident Team (ACIRT) with results provided to the asset or customer service representative. This is a common control. This control is tested under the APHIS AEI GSS.
- Operational technical safeguards to prevent data misuse begin with access control. Access to GDB information is protected by role-based access which is managed by the network firewall, network passwords, and the Oracle database. 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. At most sites, responsibility and scope of data access is defined by users' job descriptions. Policy dictates that a user may not 'self-nominate' themselves for access. Requests for access must come from their supervisor or other authorized animal health official.
- Operational audit logs are enabled within the application for defined auditable events including modification to GDB schema objects, administrative access, unsuccessful and unauthorized access attempts. Audit monitoring, analysis and reporting are implemented according to internal Standard Operating Procedures. Additional GDB and inherited AEI GSS level security controls are utilized, as delineated in the current GDB System Security Plan.

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, as identified in Section 1.1 above, 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 GDB data. GDB and AEI GSS technical security controls are delineated in the current GDB System Security Plan.

Section 9.0 Technology

9.1 What type of project is the program or system?

The Generic Disease Database (GDB) is an operational, legacy major application (MA) that collects, manages, and evaluates animal health data for disease management and surveillance programs.

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

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

Section 10.0 Third Party Websites/Applications

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 will be distributed by APHIS.

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

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

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

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

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

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

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

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

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

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

If so, is it done automatically?

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

If so, is it done on a recurring basis?

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

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

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

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

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

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

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

10.10 Does the system use web measurement and customization technology?

No.

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

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

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

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

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.

Not applicable. GDB does not use third party websites or applications. This application does not employ technology which may raise privacy concerns



Responsible Officials

Thomas Myers, VS Associate Deputy, National Animal Health Programs
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



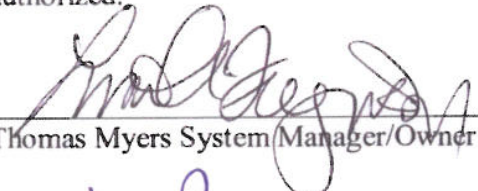
Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

(Generic Disease Database (GDB))

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.



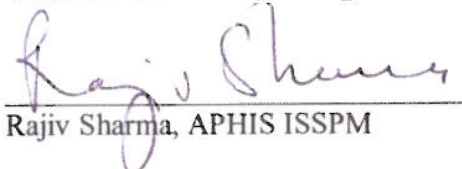
Thomas Myers System Manager/Owner Date 1/4/12



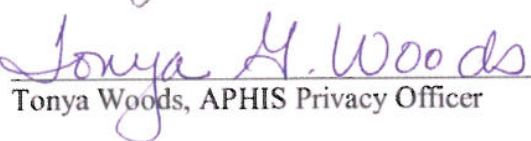
John Picanso, VS CIO Date 1-3-2012



Matthew J. McLean, Acting APHIS CIO Date 1-11-12



Rajiv Sharma, APHIS ISSPM Date 1/3/12



Tonya Woods, APHIS Privacy Officer Date 1/3/12