Privacy Impact Assessment

MIS (Management Information System)

Revision: 3

[APHIS, Wildlife Services]

Date: December, 2008

Document Information

Owner Details	
Name	Joanne Garrett
Contact Number	301-734-7921
E-mail Address	Joannne.P.Garrett@aphis.usda.gov

Revision History			
Revision	**Date**	**Author**	**Comments**
3	2/2009	Robert P. Myers	

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**

Table of Contents

1 System Information

System Information	
Agency:	Animal and Plant Health Inspection Service, Wildlife Services
System Name:	Management Information System (MIS)
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	The Animal and Plant Health Inspection Service (APHIS), Wildlife Services (WS) Management Information System (MIS) was upgraded to a direct data, online-based system in FY 2005. The new system better serves the APHIS/WS program, its customers, and the public, by improving the program's capability to monitor and measure program performance; provide timely information to decision makers, and better document APHIS/WS activities. MIS is especially important for record keeping of work in several areas of wildlife damage management related to agriculture, human health and safety, natural resources, and human property. These areas include, but are not limited to, wildlife diseases, airports, invasive species, livestock protection, blackbird damage management, and aquaculture protection. The MIS is the only data management system dedicated to tracking APHIS/WS activities and accomplishments nationwide. APHIS/WS has a strong interest in protecting the privacy of both its customers and employees as the new system is developed and maintained. To address privacy issues and to ensure protection of information provided by employees and customers, this Privacy Impact Assessment (PIA) has been developed. MIS provides a state-of-the-art data tracking and management system. It provides computer access to all APHIS/WS employees nationwide for the first time in the history of the APHIS/WS program, and enables managers to have access to valuable data at the click of a button. It assists research by enabling operations personnel to gather data that in the past could not be collected. It provides APHIS/WS employees with the capability to generate specialized reports for their cooperators without the assistance of support personnel. It facilitates better information gathering and distribution, internally for decision makers and externally for all interested parties. Implementation of this system provides e-mail capability to all APHIS/WS employees enabling better and timelier communication with the workforce.

Who owns this system? (Name, agency, contact information)	Owner: Director, Wildlife Services Operational Support Staff USDA, APHIS, Wildlife Services 4700 River Road, Unit 87, Rm. 2D-07.3 Riverdale, MD 20737-1234 Phone: 301/734-7921 FAX: 301/734-5157 E-mail: Joanne.P.Garrett@aphis.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Darlene Blaney, Director of Applications Development USDA, APHIS, Wildlife Services NRRC 150 Centre Avenue, Bldg. A, Suite 143 Fort Collins, CO 80526 Phone: 970/498-1440 Email: Darlene.G.Blaney@aphis.usda.gov
Who completed this document? (Name, agency, contact information)	Robert P. Myers, IT Staff Officer Wildlife Services Operational Support Staff Humphreys County Agriculture Center 234 West Blue Creek Road Waverly, TN 37185 PH: 301-651-8845 Email: Robert.P.Myers@aphis.usda.gov

2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	**Customer (Cooperator) Data:** This is the minimal information kept by WS which is necessary for identifying cooperators for the purpose of communication with them, and tracking of activities performed by WS employees as part of a program being conducted in collaboration with them. This usually includes a name, telephone number, mailing address, physical location address, and for cooperators for whom WS provides staff to do work on specific wildlife damage management projects, an identifying number which may be a federal tax identification number, an employer identification number, or for individual citizens who are the primary contact in a funded cooperative agreement relationship, a social security number. These identifying numbers are recorded only on the paper-based component of the system of records and are kept in WS state and regional offices in locked filing cabinets behind locked doors. These identifying numbers, including any social security numbers collected are not entered into the electronic component of MIS 2000. A required identification number is only collected for those cooperators with whom APHIS/WS implements a funded agreement. Those cooperators who receive technical assistance consisting of written advice, on-site consultation, demonstrations of methods used, training, and similar free services are not required to provide such an identifier. Information about cooperators may also include resource and resource damage information. In some instances, GPS coordinates may be recorded for locations on properties where specific damage management actions, such as wildlife disease sampling or placing of some devices. **Employee data:** This is minimal and includes name, address and telephone number of duty station, user name, password and MIS specific employee identification number. **Other data:** This may be information related to adverse human or animal incidents, indemnity, agreements, or insurance claims. Additionally, information in the system may relate to resources owned by customers which was threatened, damaged or destroyed by wildlife.

No.	Question	Response
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	☒ Yes ☐ No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	1) The Act of March 2, 1931 as amended (46 Stat. 1468; 7 U.S.C. 426-426b & 426c) 2) Debt Collection *Improvement* Act of 1996
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	☒ Yes ☐ No
4	Sources of the data in the system.	Data is generated as a result of entries made about the work performed by WS Employees. Other data is collected by voluntary submission by customers. WS purchases zip-code data from the postal service or another provider. Reference and lookup data about pesticide registration, wildlife laws and permits are obtained from Federal, State, and Local authorities.
4.1	What data is being collected from the customer?	**Customer:** name, address, phone number, customer identifying number, as applicable, and resources at risk.
4.2	What USDA agencies are providing data for use in the system?	APHIS/WS
4.3	What state and local agencies are providing data for use in the system?	Reference data about pesticide registration and wildlife laws is obtained from State and Local authorities and entered into the system by APHIS/WS users. Information about permits granted to APHIS/WS for certain types of work is also entered into the system by APHIS/WS employees. In situations where the State or local Agency is the customer, as defined under #1 above, information concerning the Agency will be obtained and entered into the system. WS users input this information. None of these agencies have access to the system. Agencies which contribute information are state wildlife management agencies, agriculture agencies, and in some cases environmental oversight agencies. Local agencies include environmental oversight agencies and city/county law enforcement agencies.
4.4	From what other third party sources is data being collected?	None
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	☒ Yes ☐ No – If NO, go to question 6.

No.	Question	Response
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	Employees will sign off on "itinerary" reports verifying their work data was entered correctly. Customers will validate all information collected about themselves before it is entered into the system. Additionally, there is review by APHIS/WS supervisors and data specialists at the District, State, Regional and National levels. Signed paper forms containing data collected from customers (cooperators) will be checked by them at signature, by the APHIS/WS employee collecting the data, and at the office which originates the data before being "approved" in the system. Field work data will be checked for completeness by the APHIS/WS employee who enters it. This electronic data entry process is monitored by an internal validation prompt system built into the MIS. Data is again reviewed for accuracy by supervisors at the APHIS/WS District and State levels.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Not Applicable
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Data of this type will be verified for accuracy, relevance, timeliness, and completeness by APHIS/WS employees in their contact with agencies and entities providing the information. Non-USDA source contributors will validate all information collected about themselves before it is entered into the system. Additionally, there is review by APHIS/WS data technicians with review privileges to verify the accuracy of the data. Relevance of data is determined by need. Only data needed to complement system processes or to provide references is acquired. Review of data as it may relate to use of it by the system is done to make determinations about its timeliness. Completeness of data is determined by verification by the contributors and an assessment by APHIS/WS as to whether it meets the purpose for which it is collected.

2.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	The information collected by APHIS-WS is necessary for identifying cooperators for the purpose of communicating with them and tracking activities performed by WS

No.	Question	Response
		employees as part of a program being conducted in collaboration with them. This includes a name, telephone number, mailing address, physical location address, and, for cooperators for whom WS provides staff to do work on specific wildlife damage projects, an identifying number which may be a Federal tax identification number, an employer identification number, or, for individual citizens who are the primary contact in a funded cooperative agreement relationship, a social security number. APHIS may also include information relating to adverse human or animal incidents, indemnity, agreements, or insurance claims.
7	Will the data be used for any other purpose?	☒ Yes ☐ No – If NO, go to question 8.
7.1	What are the other purposes?	Agency procedure requires that WS employees obtain permission to enter the property of cooperators. Information collected about cooperators will be used to document authority and license to enter premises to conduct wildlife damage management activities, pursuant to requests from cooperators for services to be conducted on their behalf. In addition, WS managers need to evaluate the effectiveness of program activities being conducted by Federal, State, and contractual personnel as program activities occur on cooperator property or on behalf of the cooperator. Information collected about the cooperator will help managers conduct such evaluations. Also in support of the APHIS mission, WS conducts surveys by selecting cooperators to provide them information about various facets of program activities related to services provided. Information provided by the cooperator during the course of business enables WS to contact them and request voluntary participation in a survey, as well as using the information volunteered by the cooperator to make determinations about how and when work will be performed, what methods will be used, and what information to provide the cooperator about the methodology, process, frequency, results, and time lines to be used in program activities, and to assist in developing safety measures and protocols.
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President	☒ Yes ☐ No

No.	Question	Response
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	☐ Yes ☒ No – If NO, go to question 10.
9.1	Will the new data be placed in the individual's record (customer or employee)?	☐ Yes ☒ No
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	☐ Yes ☒ No
9.3	How will the new data be verified for relevance and accuracy?	Not Applicable
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	**Routine use 1** permits disclosure to cooperative State government officials, employees, or contractors, as necessary to carry out the program; 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; **Routine use 2** permits disclosure 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; **Routine use 3** permits disclosure 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

No.	Question	Response
		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; **Routine use 4** permits disclosure 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; **Routine use 5** permits disclosure 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. **Routine use 6** permits disclosure to USDA employees or contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends or anomalies indicative of fraud, waste, or abuse. **Routine use 7** permits disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted

No.	Question	Response
		under 44 U.S.C. §§ 2904 and 2906.
11	Will the data be used for any other uses (routine or otherwise)?	☐ Yes ☒ No – If NO, go to question 12.
11.1	What are the other uses?	
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	☒ Yes ☐ No – If NO, go to question 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	Data consolidation is an in-house initiative in the APHIS/WS system of records until it is consolidated in the national archive as a storage process by NITC. Individuals involved in all processes are restricted to data that they are authorized to handle and the data is not exposed to any unauthorized users during this process. Standard safeguards approved by USDA for data security are used by NITC to reduce the likelihood of unauthorized access or use. Controls to protect data from unauthorized access include unique user identification, password authentication, agency implemented cybersecurity measures and firewalls installed at each access terminal, current virus protection programs updated in accordance with agency requirements and immediate lockout capability if a user is disqualified from access to data at any level. All transfer of data occurs through the agency standard virtual private network in encrypted formats. Hard copy components of the system are segregated and protected in secured and locked storage cabinets accessible only to authorized users. Other internal safeguards include monitoring of data management and development processes by the ISSM and ISSOs, and supervisory controls for field level data entry and handling activities. Data retention and disposal procedures are set by APHIS-FIRM (1999) and adhered to by APHIS/WS. These procedures further prevent unauthorized access to data which might result from data consolidation.
13	Are processes being consolidated?	☒ Yes ☐ No – If NO, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	The only process consolidation occurring in the system is that formerly manual processes for entering data have been converted to electronic entry techniques. In this change,

No.	Question	Response
		processors will remain the same and steps for data entry and creating a record will remain the same. Access controls discussed in 3a serve to prevent data from unauthorized access. Control of access to data has improved and no unauthorized access of data as a result of this change has occurred or is expected. Security is built into the application user interface. People are logged off for inactivity, and access to web-pages cannot come from outside sources. That is, the access path to each web-page is monitored.

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	☐ Yes ☒ No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	Employee information is kept active in the system as long as the individual continues to work for APHIS/WS. Information identifying cooperators is kept in the system as long as a cooperator retains an active agreement with APHIS/WS. Upon termination of employment or lapse of an active agreement, information about employees or cooperators is retained in accordance with retention schedules outlined in the APHIS Records Management Handbook (2003). NOTE: WS IS CURRENTLY CONSULTING WITH APHIS-ICM FOR LANGUAGE EXPLAINING THE RETENTION SCHEDULE FOR WS RECORDS.
14.2	What are the procedures for purging the data at the end of the retention period?	Data will be warehoused after it has been locked for at least three years. Procedures for elimination of data at the end of retention periods are performed in accordance with data elimination procedures defined in NARA data elimination guidelines (2004), the APHIS Records Management Handbook (2003) and the APHIS/WS IDMH (2004). NOTE: WS IS CURRENTLY CONSULTING WITH APHIS-ICM FOR LANGUAGE EXPLAINING THE RETENTION SCHEDULE FOR WS RECORDS.
14.3	Where are these procedures documented?	Procedures are documented at the APHIS/WS ITSC, Ft. Collins, CO. NOTE: WS IS CURRENTLY CONSULTING WITH APHIS-ICM FOR APPROPRIATE DOCUMENTATION FOR RETENTION PROCEDURES.

No.	Question	Response
15	While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	Employees and their supervisors verify the accuracy, relevance, timeliness and completeness of data routinely. Monthly, quarterly, and annual reviews of much of the data are conducted, and employees verify the data about cooperators with those cooperators annually.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No

2.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	☒ Yes ☐ No – If NO, go to question 18.
17.1	How will the data be used by the other agency?	No other agencies will have direct access to the MIS, but data contained in records of the system may be shared with other agencies in the course of business and for implementing collaborative program activities and objectives. Agencies which collaborate with APHIS/WS in implementation of, or Agencies which regulate, wildlife management activities, or who have an interest, or regulate, in animal or public health, or national security may request data in the MIS to be shared. Data may be shared with State or Federal government-level representatives of the Environmental Protection Agency as part of APHIS/WS' responsibility to comply with the Federal Insecticide Fungicide and Rodenticide Act (U.S. Code Title 7, Section 136i-1). Information transferred to agencies will be used to identify and verify management actions performed by APHIS/WS under funded interagency agreement(s), Memoranda of Understanding(s), and / or permits issued by the agencies. Some data provided to land management agencies, such as the Bureau of Land Management (BLM) and the Forest Service (FS), where a cooperator has a grazing allotment also require information about wildlife damage management actions performed on the agencies managed lands. APHIS/WS has memoranda of understandings, or other official agreements, with such agencies for the purpose of wildlife damage management on lands controlled by them and have agreed to report wildlife

No.	Question	Response
		damage management actions to them. This consists of information about a cooperator's resources which are being protected by a APHIS/WS action. Wildlife is a publicly owned resource and is managed by both Federal and State agencies. APHIS/WS provides informational data to the appropriate agency to demonstrate compliance with statutes, rules, regulations, orders, or permits issued by the agency. Examples include APHIS/WS activities that involve Federal and State managed and regulated wildlife species. Data concerning the locations where APHIS/WS management actions occurred can be used by the agency to improve overall management of the species. Information shared with other federal agencies may be used to monitor wildlife population health, human health, wildlife disease outbreaks, or potential national security issues related to the release or propagation of wildlife diseases which may be zoonoses for human populations, or diseases which may threaten food supplies of the United States. Information is provided to the EPA, and their agents in each State, regarding where registered pesticides are applied pursuant to APHIS/WS wildlife damage management programs. This data sharing documents compliance with the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) (U.S. Code Title 7, Section 136i-1). EPA uses this information to fulfill its federal reporting requirements under FIFRA.

No.	Question	Response
17.2	Who is responsible for assuring the other agency properly uses the data?	APHIS/WS is responsible for the protection and proper use of the data within the MIS. APHIS/WS restricts access to data by other agencies based on a "need to know" rule for the agency, the office or program of the agency, and the identity of the individual who receives the data. An agency's need to know is established through interagency agreement(s), Memoranda of Understanding(s), statute(s), rule(s), regulation(s), or order(s) issued pursuant thereto. Furthermore, release of data is pursuant to the uses identified within the Privacy Act and the routine uses identified by APHIS/WS for the records maintained in the MIS. APHIS/WS releases the data with the understanding that the other agencies are bound by the regulations of the Privacy Act through which the data was originally released. Once this information is conveyed to representatives of the other agencies, APHIS/WS assumes no further responsibility, but documents a record of custody which identifies the office of the agency, and individual, which received the data.
18	Is the data transmitted to another agency or an independent site?	☒ Yes ☐ No – If NO, go to question 19.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	Memoranda of understandings and official communication records regarding transfer of data are kept by APHIS WS to document the interconnection of between APHIS WS and those agencies/entities receiving data. In addition, information and warnings about protecting PII and or Privacy Act protected data are provided during the transfer.
19	Is the system operated in more than one site?	☒ Yes ☐ No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	Paper records related to Agreements for Wildlife Damage Management are kept at State APHIS WS offices where relationships with customers are created and maintained. Some data in these records also exist as electronic entries in the electronic component of the system. The data entries within the electronic component are exact duplicates of those in paper records and any business rules are in place that require updating of the electronic component when any changes occur in the paper component. Beyond this dual process, the system is not operated at more than one site, but exists as an electronic direct data entry process online.

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	Access to data in MIS is determined by the data usage role of the APHIS/WS employee which is determined by duties. Within the agency, access both as to limits and authority are compliant with APHIS "least privilege" rule (APHIS Directive 3140.5), for which policy is established further in APHIS/WS Directive 4.120 and detailed guidance is provided in the APHIS/WS Information and Data Management Handbook (IDMH) (2008). APHIS/WS employees authorized to access data at any level are collectively referred to in this document as **users**. Access to data in the system is limited to APHIS/WS personnel only and includes: APHIS/WS Deputy Administrator APHIS/WS system owner and/or designees USDA-OCIO-National Information Technology Center APHIS/WS Information System Security Manager (ISSM) and / or designees APHIS/WS Information System Security Officer (ISSO) and / or designees APHIS/WS headquarters MIS liaison APHIS/WS data developers APHIS/WS system administrators APHIS/WS system manager APHIS/WS operational program managers APHIS/WS operational program data technicians APHIS/WS operational program field specialists APHIS/WS office administrative staff

No.	Question	Response
21	How will user access to the data be determined?	Individual employees within APHIS/WS have limited access to some data based on their roles in the agency. A few individuals have access to all data, while most have limited access. Criteria and procedures, controls, and responsibilities regarding access are documented in APHIS/WS Directive 4.120 and the APHIS/WS Information and Data Management Handbook. Each user has his/her account, and password to the system. Accounts are given according to each state's individual policy. Within the system, each user has a specific role, determined at the State levels but codified and documented by the Working Group, as to how much data can be accessed. The different roles, such as User, District Supervisor, State Director, and Data Technician, are controlled by the database software (Oracle).
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ No
22	How will user access to the data be restricted?	User access to data is restricted to data necessary for the user's job. The following describes the role and access of users of the MIS system of records: The **APHIS/WS Deputy Administrator (DA)** oversees the MIS System of Records as part of the total oversight of the APHIS/WS National Program. The role of this position is programmatic supervisor of the system owner. Data in the system will not be accessed by the DA directly, but through the system owner, the ISSM, a designated ISSO or the headquarters MIS liaison. The **system owner**, who is the APHIS/WS Operational Support Staff Director, will work closely with ISSMs and ISSOs to ensure an effective ISS program. The role of the system owner is to provide supervisory oversight and administrative collaboration to the Information Technology Support Center (ITSC) management staff and provide input to the APHIS/WS Management Team regarding the MIS system of records. Duties also include oversight of the creation (or receipt), maintenance and use, and disposition of records in the system. The system owner will not access data directly, but through the ISSM, a designated ISSO, or the Headquarters MIS Liaison. Access by the system owner will be determined by a need to monitor or evaluate system integrity, efficiency, or general function, to evaluate various aspects of data handling or content, or to provide

No.	Question	Response
		programmatic input about overall or component program activities with cooperators. **USDA's National Information Technology Center (NITC)**, administered by the USDA Office of the Chief Information Officer (OCIO) provides data management services to APHIS/WS for its MIS system of records. The OCIO's, assistants and/or designees who work at the NITC facility servicing APHIS/WS function as neutral users of APHIS/WS data. Their duties and responsibilities include handling of APHIS/WS data in accordance with standards established by NITC and APHIS/WS, continuous storage management, security administration, regular dataset backups, contingency planning/disaster recovery, and technical support. Access by individual employees at NITC is restricted to the need for implementing these actions, as assigned. NITC has established best management practices which include approved security measures for the protection of data of its clients. NITC managers collaborate with the APHIS/WS ISSM and her/his designees in handling and storage of APHIS/WS data. **The Information System Security Manager (ISSM)** is the Director of the APHIS/WS ITSC, is appointed by the System Owner, and is responsible for all security oversight of the electronic component of the MIS system of records. The ISSM appoints ISSOs and defines duties and security responsibilities for all APHIS/WS ITSC personnel who are users of the system. The ISSM collaborates with APHIS security experts and other APHIS/WS managers to develop security systems, protocol, and practices to protect the MIS system of records. The **Information System Security Officer(s) (ISSO)** are appointed or assigned ISSO duties by the ISSM and are responsible for ensuring that security measures are implemented and maintained within their area(s) of responsibility. Their duties include routine monitoring of MIS data entry, tabulation, storage, and retrieval within their areas of responsibility and providing prescribed reports in appropriate formats to the ISSM and other approved requesters. Access to data in the system is determined by the need of these officers to adequately monitor the use of the system within their purview. ISSOs may be granted access to the entire system of records by the ISSM for specific official duties necessitating this level of access. Access to data in the system by the

No.	Question	Response
		headquarters **MIS liaison** is determined by the need for compiling reports or providing data related to operational and research program activities and accomplishments. The MIS liaison provides a diversity of reports and information to headquarters and operational and research managers about specific projects or their results on a state or national level. Verification of the accuracy of data about wildlife damage management or research activities for national reports comprising a compilation of all state reports is the responsibility of the MIS liaison. Only rarely will this individual require access to privacy information contained in the system, however. Access to data by **system administrators** is determined by the need to effectively perform tasks related to overall protection, troubleshooting, and modifications to programs and equipment that store the data. Although the administrator does not need access to view specific information about people in the database, duties do require access to all data in order to evaluate system integrity, efficiency, and function. The **system manager**, who is the MIS Working Group Chair, will participate in systems management by steering a working group in reviewing, updating, developing and maintaining policy and procedures for use of the system, collaborating with the MIS Center staff about system modifications, and acting as consultant to the APHIS/WS Management Team regarding MIS. Occasional access to data in the system is required in order to monitor quality of data entry and management. Access by **system developers** is based on the need to examine the nature of data being input and stored to determine formats and structures for capturing, storing and relating the data. Because improvements will be made to the system on an ongoing basis, input and output data will be available to system developers for stress testing and improving the overall function of the system and its software components. Access by **program managers** in APHIS/WS will be tiered based on the level of management occupied. District level managers of operational programs have access to all data related to their districts. State level managers have access to all data about their state operational program, while regional managers have access to data about their regional program. State, district, and regional managers also have access, through case-by-case approval by the state-level manager where specific data was collected, or

No.	Question	Response
		by the headquarters MIS Liaison, for national level data, or to other state and national program information. **Operational program data technicians** will access data at the state program level for the purpose of providing reports upon request to various APHIS/WS managers, field employees, and other authorized requesters. Additionally, they will access their state's data in the system based on the need to assist in the process of error checking, validating, and consolidating data. Their access will be authorized by the incumbent State Director of the state-level program where they are employed. Operational program **field specialists'** access is determined by the needs demanded by role. This level of access is usually determined by the requirements for individual input of data generated when the employee records the results of work, by the need to validate input data, the need to provide information to cooperators about their projects, and the need to report to supervisors about details of work. Access of this nature is limited to viewing data input by the individual employee, and reports that are generated by the system. For special needs, the State Director may grant access to other data entered by other employees in the state. This access is read-only except where two or more specialists are working on one project and need to collaborate in the entry of data. Some **APHIS/WS office administrative staff** of district, state, regional, and national offices handle various data components. Most of these are hard copy documents for local file management. Access to the system for these staff members is limited to routine handling of such documents, except instances where the State Director authorizes data entry by these employees for specific purposes germane to state program goals. Some administrative personnel function as public contact specialists and provide information to requesters. They will collect information from such requesters and enter it into the system. They have access to only their input data for error checks and validation.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	☒ Yes ☐ No

2.6 Customer Protection

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	The WS Information System Security Manager (ISSM) and his/her Information System Security Officer(s) (ISSO)
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	Customers have an assigned a contact person who is an employee of WS. They are instructed to contact the ISSM through these contact personnel when questions or issues arise. Employees are authorized to contact their State/Regional WS MIS Data Technician who handles issues or questions related to privacy rights. WS has a national/ headquarters-level Privacy Officer who may also be contacted directly regarding privacy questions or issues.
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	☒ Yes – If YES, go to question 27. ☐ No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	
27	Consider the following: ▪ Consolidation and linkage of files and systems ▪ Derivation of data ▪ Accelerated information processing and decision making ▪ Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	☐ Yes ☒ No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	
28	How will the system and its use ensure equitable treatment of customers?	The system provides the necessary data about a customer to allow employees who work directly with them to be able to best assess and provide service to them, as needed. Equally complete data about each customer will enhance equitable treatment.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	☐ Yes ☒ No – If NO, go to question 30
29.1	Explain	

3 System of Record

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	☒ Yes ☐ No – If NO, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	Data may be retrieved by the name of the cooperator as it appears in agreements with WS. Employee data may be retrieved using the employee name.
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov.)	3410-34-P
30.3	If the system is being modified, will the SOR require amendment or revision?	☐ Yes ☒ No

4 Technology

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	☐ Yes ☒ No – If NO, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	

5 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE FOR CYBER SECURITY.

Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

_____
(System Name)

This document has been completed in accordance with the requirements of the E-Government 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.

_____ _____
System Manager/Owner Date
OR Project Representative
OR Program/Office Head.

_____ _____
Agency's Chief FOIA officer Date
OR Senior Official for Privacy
OR Designated privacy person

_____ _____
Agency OCIO Date