Privacy Impact Assessment
Management Information System 2000 (MIS2000)

- Version: 1.5
- Date: October 5, 2017
- Prepared for: USDA OCIO TPA&E

Privacy Impact Assessment for the

Wildlife Services Management Information System (MIS2000)

October 5, 2017

Contact Point
Jason Zebell
APHIS, Wildlife Services
(970) 498-1444

Reviewing Official
Danna L. Mingo
USDA-APHIS
United States Department of Agriculture
(301) 851-2487

Abstract

This Privacy Impact Assessment (PIA) is developed for the USDA APHIS Wildlife Services (WS) Management Information System (MIS) 2000. MIS has been implemented as a system of records for documentation and tracking of business conducted by Wildlife Services in its operational program in cooperative relationships with government, business/industry, and private individuals. This PIA is being conducted to both report to government and the public about the system, and to evaluate the system's conformity to privacy and information collection mandates.

Overview

The Animal and Plant Health Inspection Service (APHIS), WS MIS system was built to better serve 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 work.

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 work 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.

MIS provides a data tracking and management system and it 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.

A typical transaction in MIS occurs when WS employees enter information related to wildlife damage management projects conducted by them in the field. This information may include data about direct damage management work or technical assistance projects.

While WS provides no direct access to the system or its components to other entities, the Wildlife Services program does share some information collected by employees and entered

into the system. This sharing is a manual process and maybe be shared on an excel spreadsheet. This may include:

- Agencies which collaborate with APHIS/WS in implementation of, or Agencies which regulate, wildlife management projects/programs, or who have an interest, or regulate, in animal or public health, or national security may request data in the MIS to be shared.
- 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).
- 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.

This system of records features a companion module for tracking pesticide usage by WS, the Control Materials Inventory Tracking System (CMITs). This module accommodates data entry about the use of chemical applications and inventories.

Authority for maintaining MIS as a system of records resides in The Act of March 2, 1931 as amended (46 Stat. 1468; 7 U.S.C. 426-426b & 426c) and Debt Collection Improvement Act of 1996

1 Section 1.0 Characterization of the Information

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

The following information is collected and maintained/updated 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 work 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 specific wildlife damage management projects. 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, and MIS unique employee identification number generated by the system.
- Other data: Information in the system may relate to resources owned by customers which was threatened, damaged or destroyed by wildlife.

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

Data is generated as a result of entries made about the work performed by WS Employees. Other data is collected by WS through voluntary submission by customers that may include verbal communication. This data is entered into the system by WS employees. Reference and lookup data about pesticide registration, wildlife laws and permits are obtained from Federal, State, and Local authorities.

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

The information collected by APHIS-WS is necessary for identifying cooperators for the purpose of communicating with them and tracking work performed by WS employees as part of a program being conducted in collaboration with them. This includes a name, telephone number, mailing address or physical location address.

Information is also collected because 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 work, pursuant to requests from cooperators for services to be conducted on their behalf. In addition, WS managers need to evaluate the effectiveness of program work being conducted by Federal, State, and contractual personnel as program actions 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 work 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 work, and to assist in developing safety measures and protocols.

1.4 How is the information collected?

Information is collected for the system through direct contact by WS employees with cooperators. They collaborate with cooperators in filling out forms which contain the information. These forms exist in the electronic component of MIS or are paper forms.

Other information is collected from WS employees who have direct knowledge about operational work performed, and information about themselves.

Some information is collected about wildlife and wildlife damage management subjects from sources made available by local, state, or federal government entities, or is general information published on the web.

1.5 How will the information be checked for accuracy?

Employees validate information through a screen review process before permitting its entry into the system. Customers will validate all information collected about themselves on the APHIS form 12 and then signing it to agree that the information is accurate. 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.

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.

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

The following legal authorities require collection of certain information in MIS:

1) The Act of March 1931 as amended (46 Stat. 1468; 7 U.S.C. 426-426b & 426c)
2) Debt Collection Improvement Act of 1996

In addition, WS enters into agreements with cooperators in the private and public sectors in which such cooperators agree by signature to submit the information collected. The agreements include Memoranda of Understandings, Memoranda of Agreements, Cooperative Service Agreements, and Cooperative Service Field Agreements.

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

Privacy information collected about WS employees and cooperators is protected through a number of mitigation efforts that include information access control, and system protocols. Data consolidation has the potential to create privacy risks, however, data consolidation in MIS is an in-house initiative in the APHIS/WS system. 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 to reduce the likelihood of unauthorized access or use.

Other controls to protect data from unauthorized access include unique user identification, eAuthenitication, 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.

2 Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

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 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 under 44 U.S.C. §§ 2904 and 2906. 2.2

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

WS performs simple analyses of consolidated results of direct control and technical assistance activities. Microsoft Access and Microsoft Excel are used. Analyses include simple descriptive statistics and data showing trends in wildlife damage management effects, wildlife damage impacts, and results of work. No personal data about cooperators is subjected to analysis since data sets used are stripped and consolidated. Managers in WS may use data about hours worked by field employees to analyze time spent on projects or other efficiency metrics related to field work or technical assistance projects.

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

Reference and lookup data about pesticide registration, wildlife laws and permits are obtained from Federal, State, and Local authorities and are used to populate entries about wildlife damage management work, or to provide reference material for employees making data entries.

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.

Analyses are done by request from WS supervisory staff or other entities who have requested such information through official channels. Such information is purged of any

privacy information and is checked to ensure that outputs do not point to private individuals or their information.

Lookup and reference information is used only by those who have been approved by the ISSM and entries of lookup data are automated to provide unaltered data.

3 Section 3.0 Retention

3.1 How long is information retained?

Information in the MIS2000 System is permanent until the disposition authority is approved by NARA. The proposed schedule is as follows:

Information is retained about employees as long as they are actively employed by the unit, or as long as their project-related work history is kept in the system. Information is retained about cooperators as long as agreements are active or their work history is kept in the system. Reference and lookup information is kept in the system as long as it is used by employees to populate record material. In general, records are retained in accordance with data elimination procedures outlined by NARA guidelines, APHIS records management guidelines and the APHIS/WS Information and Data Management Handbook (IDMH).

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

No (Pending Approval)

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

Since data may be kept too long or not long enough, WS records management personnel review record schedules and disposition procedures intermittently to ensure that outdated records are purged or moved to archived files as needed. In addition, almost all data about employees and cooperators is reviewed annually for accuracy, timeliness, and relevance as part of the WS business processes in place, making a business policy practice to be an assurance that records will be reviewed routinely and updated/purged as needed.

4 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?

Data may be shared with the USDA Office of General Counsel if it pertains to a legal process, litigation actions that are brought by WS, or by entities in the private sector. Other investigatory units within USDA may be provided access to some data if an investigation of waste, fraud, or abuse, or investigation of misconduct by a WS employee is implemented.

4.2 How is the information transmitted or disclosed?

Information transmitted or disclosed to USDA is provided through the WS FOIA coordinator in the format and process defined by the department in conformity to USDA FOIA process.

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

Privacy risks associated with internal sharing are mitigated through handling procedures which ensure that information released is only what is requested, is legally allowed to be released, and is securely passed directly to the authorized recipient or their official agents.

5 Section 5.0 External Sharing and Disclosure

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

Information is shared with the following external organizations. Purposes are declared:

Environmental Protection Agency – names, addresses, physical locations and pesticide application performed for selected cooperators as part of submission of pesticide application work and types

U.S. Treasury Department – names, addresses, social security numbers or Tax ID numbers of delinquent cooperators, in compliance with the Debt Collection Improvement Act.

National Archives and Records Administration – Paper Records – Compliance with record keeping regulation and policy.

Department of Justice – Cooperator information and details about work done for them – in response to court requirements surrounding lawsuits against WS.

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.

The sharing of personally identifiable information outside USDA is compatible with the original collection and is covered by routine uses declared in the WS SORN Docket No. APHIS-9 Wildlife Service Management Information System

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

Information shared and transmitted outside USDA may be done by direct contact, or through email, standard mailing procedures, or in some instances by phone. Rules and guidance for protection of such shared information is provided in Sections 3.7 and 6.0 of the WS Information Data Management Handbook (IDMH). Email transfers have warning disclaimers attached which notify recipients about security considerations and instruct recipients who erroneously receive such transmissions to delete them.

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

A potential risk to information resulting from external sharing would be transmittal of unauthorized material or transmittal to wrong parties. WS uses a policy-controlled, tiered approval process that ensures evaluation of all aspects of the transmittal process to validate the appropriateness and legality of such information transfer.

6 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?

Yes

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

Yes

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

Individuals have the opportunity during the collection process to review uses that may be made of the information and declare and document special considerations related to use of information.

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.

Upon request for information from contributors, WS provides an information sheet defining the uses to be made of any submissions. To mitigate risks that individual contributors might be unaware of the collection, the use and purpose of the collection is discussed by WS employees and questions by the contributor are encouraged.

7 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?

Under the Privacy Act (PA), a person may seek access to records that are retrieved by his/her own name or other personal identifier, such as social security number or employee identification number. Such records will be made available unless they fall within the exemptions of the PA or the Freedom of Information Act (FOIA).

Your request must be in writing. Indicate that you are making a request under the PA. Address the request to the following address:

- VIA MAIL:

Animal and Plant Health Inspection Service

Director, Freedom of Information and Privacy Act Staff

4700 River Road, Unit 50

Riverdale, MD 20737

- VIA E-MAIL: foia.officer@aphis.usda.gov

NOTE: While e-mail attachments are often an important and legitimate means of conducting business, they also have the potential to cause great harm to our e-mail infrastructure, as well as to individual workstations. Please place the text of your PA request into the 'body' of the email message.

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

Customers may correct inaccurate or erroneous information by submitting a Privacy Act request to: APHIS FOIA Office, 4700 River Road, Unit 50, Riverdale, MD 20737 or email the FOIA Officer at FOIA.Officer@aphis.usda.gov. APHIS employees can update contact information through the Address Book Tool, which updates the Enterprise Active Directory (EAD) and in turn updates the APHIS ServiceNow profile. External customers' information is corrected through communication via the Helpdesk.

Data in the APHIS ServiceNow system is protected by access controls.

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

Procedures for correcting information in the system can be found in the APHIS-9 Wildlife Service Management Information System SORN.

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

N/A

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

There is some risk that the contributor's information would fail to be corrected by initial processes, but the multi-level redress alternatives available to the contributor makes this outcome extremely unlikely. There is also a limited risk that the corrected privacy information

could also be erroneous, but documentation to the contributor from WS ensures that the corrected information is available for review and approval by the contributor.

8 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?

Procedures in place to determine which users may access the system include unique user identification, two-factor authentication (eAuth), agency implemented cybersecurity measures, and firewalls installed at each access point. When employees are disqualified from access to the system or any sector of the data, there is an immediate lockout capability. Documentation of procedures are available in the MIS2000 Rules of Behavior and MIS2000 Security Features User's Guide in the WS IDMH as appendices.

8.2 Will Department contractors have access to the system?

Yes.

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

Users are required to take annual departmental/agency privacy training. All new users are also given orientation by the ISSM, ISSM representatives, or supervisors on protecting privacy in the WS system of records.

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

Yes

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

The system automatically records an audit trail which identifies logon and data change or data entry actions. Routine monitoring of audit records is done.

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

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

There is a very slight risk that WS field employees could gain access to privacy information, such as names and addresses of cooperators which they do not service. However, access to accounts by non-servicing employees must be granted by security personnel and by supervisors of both the servicing employees and those employees seeking access. Further, any access to privacy data in the system is only available to certain WS personnel and that by use of the least privileged rule.

9 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?

A web-based direct data entry system of records.

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

Because this project is web-based, there is some risk that unauthorized intruders could gain access to privacy information. However, the system resides behind the APHIS firewall, and is protected by eAuthentication access protocols. Users are granted initial access through a tiered approval process which provides layers of validation, and only employees supervised by WS can become users with access into the system.

10 Section 10.0 Third Party Websites/Applications

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

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

Yes

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

WS does not use 3rd party websites or applications for conducting business or contact initiatives.

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

N/A

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

N/A

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?

N/A

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

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

N/A

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?

N/A

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)?

N/A

10.10 Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

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

N/A

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.

N/A

Approving Officials

Lewis E. Klaus

System Owner

United States Department of Agriculture

Rajiv Sharma

APHIS ISSPM

United States Department of Agriculture

Tonya Woods
APHIS Privacy Act Officer
United States Department of Agriculture