Privacy Impact Assessment
Operations and Reporting System (OARS)

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: July 6, 2021
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

Wildlife Services Operations and Reporting System (OARS)

July 6, 2021

Contact Point

David Reinhold
USDA APHIS Wildlife Services
301-851-4002

Reviewing Official

Tonya Woods, APHIS Privacy Act Officer
USDA APHIS
301-851-4076

Abstract

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

Overview

As part of the modernization effort, the Animal and Plant Health Inspection Service (APHIS), WS OARS application system is built based on a cloud solution 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.

The OARS WS users will have the option of using a desktop component or a mobile application. Both the front end mobile and desktop components will be synced via a layer of support services that also handles the program logic.

OARS 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 current system of record, 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.

OARS will serve a data tracking and management system and it will enable managers to have access to valuable data at the click of a button. It assists program management 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 OARS occurs when WS employees enter information related to wildlife damage management projects they conduct 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 WS program does share some information collected by employees and entered into the system. This sharing is a manual process and may be 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 OARS 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.

The OARS 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 OARS as a system of record resides in the Act of March 2, 1931 as amended (46 Stat. 1468-69; 7 U.S.C. §§ 8351-8352) and The Act of December 22, 1987 (Public Law No. 100-202, § 101(k), 101 Stat. 1329-331, 7 U.S.C. § 8353).

Section 1.0 Characterization of the Information

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

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

The 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, email address, physical location address, and specific wildlife damage management projects. Information about cooperators may also include resources and property that were threatened, damaged, or destroyed by wildlife, values of resources or property and adverse human or animal incident 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, username, and OARS 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 personal communication. This data is entered into the system by WS employees. Reference and lookup information about pesticide registration, wildlife laws and permits are obtained from federal, state, and local authorities. A geodatabase containing publicly available land ownership and property boundary maps will be procured from a third-party commercial provider and linked to the system.

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, email 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 contractor 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 gathers information from cooperators 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. WS employees gather information from cooperators and enter information directly into OARS using electronic forms, or on paper forms that are subsequently entered into OARS.

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 WS FORM 12A and then sign 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. The APHIS WS employee collecting the data will be reviewed by another WS employee 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 OARS. 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 OARS:

1) The Act of March 2, 1931 as amended (46 Stat. 1468-69; 7 USC §§ 8351-8352); and
2) The Act of December 22, 1987 (Public Law No. 100-202, § 101(k), 101 Stat. 1329-331, 7 USC § 8353) 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 OARS 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, e-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's standard virtual private network (VPN) 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.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

OARS will support WS' mission to provide services necessary to manage wildlife damage to protect agriculture, natural resources, property, and human health and safety. These areas include but are not limited to wildlife diseases, airports, invasive species, livestock protection, blackbird damage management, and aquaculture protection. The WS Program supports the APHIS mission to safeguard the health, welfare, and value of American agriculture and natural resources. APHIS and WS will use OARS to maintain a record of activities conducted by program personnel and cooperators pursuant to its mission and responsibilities. OARS will serve as a data tracking and management system and it will enable managers to have access to valuable wildlife damage management data. It provides WS personnel with the capability to generate specialized reports for their cooperators. It facilitates better information gathering and distribution, internally for decision makers and externally for all interested parties. Additionally, collected information will be used to generate wildlife damage management reports for the general public and agency stakeholders. Reports made available to the general public will not contain personal identifying information or distinguishable locations disclosures. APHIS WS has a statutory requirement to protect the privacy of both its customers and employees. OARS will also include a Control Materials Inventory Tracking System (CMITS), used for tracking the inventory and WS' usage of pesticides, pyrotechnics, explosives and other restricted items.

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

WS uses a suite of analytical tools including statistical software, database management, spreadsheets and geospatial tools to analyze program data. Analyses include 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.

OARS will integrate commercially available geospatial products depicting land ownership and property boundaries of public and privately owned lands (parcel data). This parcel data is publicly available at the county level but is curated by commercial vendors to provide single source national level data. The maps will be used to identify properties where the Program has permission to conduct wildlife damage management. Parcel data will not be made available to the public.

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.

Section 3.0 Retention

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

3.1 How long is information retained?

Information in the OARS is permanent until the disposition authority is approved by NARA.

In November 2020, APHIS Records Management submitted WS' retention schedule for the current System of Record, MIS2000, to NARA. The request was returned without actions. On June 23, 2021, APHIS emailed NARA requesting what actions need to be accomplished for schedule approval. Once completed and approved OARS will replace the legacy system MIS2000, as the official system of record.

The proposed schedule is as follows:

a. Customer data, both paper and electronic, is collected personally and may be entered into the system.

(Customer data is information about the cooperator including mailing address, phone number, number of acres, and resources protected.)

Personal Customer data will never be collected in a field journal. Fieldwork data maybe collected in a field journal but is required to be destroyed after input into the System of Record.

Disposition: Electronic. Updated by consultation with customer while account is active. (Information is updated in the system continually while the employee works with the cooperator regarding the management of wildlife damage and resources to be protected.)

b. Employee data entered directly into the system.

Disposition: Updated at least annually by employees. Data records cutoff is at the end of the FY in which the case or project file is closed or by expiration date on document. Destroy 5 year(s) after cutoff (If approved by NARA).

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. 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.

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

In November 2020, APHIS Records Management submitted WS' retention schedule for the current System of Record, MIS2000, to NARA. The request was returned without actions. On June 23, 2021, APHIS emailed NARA requesting what actions need to be done for schedule 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.

Private data information is only accessible to personnel working on that particular project or property. When the project is complete or services are no longer required, OARS data managers remove personnel access to the private information. The risk to private data while the project is active is low.

Section 4.0 Internal Sharing and Disclosure

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

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

WS Program personnel will be able to generate reports using information from OARS. No other USDA organization will have direct access to the system except APHIS Market and Regulatory Programs Information Technology (MRP IT) – To resolves software issues.

Reports generated for USDA organizations using information from OARS include:

- USDA Natural Resources Conservation Services (NRCS) – Cooperative Feral swine damage management information. The agency partnership authorized by the 2018 Farm Bill.
- USDA Office of General Counsel if it pertains to a legal process or litigation actions.
- USDA Farm Services Agency- Information may be provided to FSA under the Livestock Indemnity Program (LIP).

4.2 How is the information transmitted or disclosed?

WS transmits/discloses PDF or read only web display to USDA 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.

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.

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?

1) To cooperative federal, state, local, and tribal government officials, employees, or contractors, and other parties 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;
2) To federal, state, tribal, and local regulatory agencies and their employees and contractors who collaborate with WS in implementation of, or agencies that regulate, wildlife management projects or programs, or who have an interest in, or regulate, animal or public health, wildlife species conservation, or national security;

3) To land management agencies, such as the Bureau of Land Management, the U.S. Fish and Wildlife Service, U.S. Forest Service, U.S. Department of Defense, and state, local, and tribal land management programs relating to, but not limited to, wildlife damage on grazing allotments, recreational lands (parks), and property; species conservation projects; or disease surveillance;
4) To consumer reporting agencies in accordance with section 31 U.S.C. 3711(e);
5) To state or federal government-level representatives of the U.S. Environmental Protection Agency, in compliance with the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) mandate (FIFRA Sec. 8, 7 U.S.C. 136f, and FIFRA 7 U.S.C. 136i-l), of the location on a cooperator's property where certain regulated pesticide devices are deployed or regulated pesticides are applied;
6) To cooperating laboratories, federal, state, and local government officials, employees, or contractors, and other parties engaged to assist in administering animal health programs to assist the agency in carrying out the program.
7) To USDA contractors or cooperators with signed agreements collaborating with USDA in conducting, managing, or evaluating wildlife disease or pest surveillance or control programs, and monitoring for animal issues, diseases, or pests or to aid in containing and responding to a foreign or domestic animal disease outbreak, zoonotic disease outbreak, bioterrorism, radiological event, or other animal health emergency;
8) To a congressional office in response to an inquiry from that congressional office made at the written request of the individual about whom the record pertains;
9) To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for USDA, when necessary to accomplish an agency function related to this system of records.
10) To the Department of Justice when: (a) USDA, or any component thereof; or (b) any employee of USDA 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 (c) the United States Government, is a party to litigation or has an interest in such litigation, and USDA determines that the records are relevant and necessary to the litigation and the use of such records by the Department of Justice is for a purpose that is compatible with the purpose for which USDA collected the records;
11) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when USDA or other Agency representing USDA determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;
12) To appropriate agencies, entities, and persons when: (a) USDA suspects or has confirmed that there has been a breach of system of records; (b) USDA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, USDA (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

13) To appropriate law enforcement agencies, entities, and persons, whether Federal, foreign, State, Tribal, local, or other public authority responsible for enforcing, investigating, or prosecuting an alleged violation or a violation of law or charged with enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, when a record in this system on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, or rule, or court order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutive responsibility of the receiving entity;
14) To another Federal agency or Federal entity, when information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach;
15) To USDA contractors, partner agency employee or contractors, or private industry employed to identify patterns, trends, or anomalies indicative of fraud, waste, or abuse; and
16) To the National Archives and Records Administration (NARA) or to the General Services Administration for records management activities 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.

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 and Operations and Reporting 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 encrypted 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 unauthorized 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.

Section 6.0 Notice

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

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

Yes. Wildlife Services, Management Information System and Operations and Reporting System. (pending new SORN approval)

A new SORN covering the old system of record MIS2000 and OARS is under development. The MIS2000 SORN is available.

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

Yes

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

Yes

6.4 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.

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

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.

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?

§1.112 Procedures for requests pertaining to individual records in a record system.

(a) Any individual who wishes to be notified if a system of records maintained by an agency contains any record pertaining to him or her, or to request access to such records, shall submit a written request in accordance with the instructions set forth in the system notice for that system of records.

Under the Privacy Act (PA) of 1974 (5 U.S.C. §552a), a person may seek access to records that are retrieved by his/her own name or other personal identifiers, 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 FACSIMILE: 301-734-5941

VIA E-MAIL: APHISPrivacy@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.

The USDA Privacy Policy can be located at the following:

URL: https://www.usda.gov/privacy-policy

Information about FOIA requests can be found at:

https://www.aphis.usda.gov/aphis/resources/lawsandregs/privacy-act/privacy

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 Privacy Act Office, 4700 River Road, Unit 50, Riverdale, MD 20737 or email the Privacy Act Officer at APHISPrivacy@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.

The USDA Privacy Policy can be located at the following URL:

https://www.usda.gov/privacy-policy.

Information about FOIA requests can be found at:

https://www.aphis.usda.gov/aphis/resources/foia/ct_how_to_submit_a_foia_request

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 or

https://www.aphis.usda.gov/aphis/resources/foia/ct_how_to_submit_a_foia_request

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.

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 – SiteMinder), 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. Prior to the OARS going live, documentation of procedures will be available in the OARS Rules of Behavior and OARS 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?

No, it is currently beginning its initial Certification and Accreditation (C&A) to obtain its Authority to Operate (ATO).

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.

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 and mobile-app 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 online-based application with web and mobile components, 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.

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?

N/A

If so, is it done automatically?

N/A

If so, is it done on a recurring basis?

N/A

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?

N/A

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?

N/A

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

N/A

10.12 <u>Privacy Impact Analysis</u>: 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

Responsible Officials

David S. Reinhold, Director WS OSS
System Owner

Steve Kendrot, Deputy Director WS OSS
Product Owner

Approval Signature

PRESTON GRIFFIN
Digitally signed by PRESTON GRIFFIN
Date: 2021.07.09 12:19:26 -04'00'

MRP-IT ISSPM
Animal and Plant Health Inspection Service
United States Department of Agriculture

JANELLE JORDAN
Digitally signed by JANELLE JORDAN
Date: 2021.07.13 09:01:41 -04'00'

APHIS Privacy Act Officer
Animal and Plant Health Inspection Service
United States Department of Agriculture

DAVID REINHOLD
Digitally signed by DAVID REINHOLD
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=DAVID REINHOLD, 0.9.2342.19200300.100.1.1=12001000092406
Date: 2021.07.07 12:39:49 -04'00'

David S. Reinhold
APHIS WS Director OSS
System Owner
United States Department of Agriculture.