

Privacy Impact Assessment Integrated Plant Health Information System (IPHIS)

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: March 11, 2020
- Prepared for: USDA OCIO-Policy,
E-Government and Fair Information
Practices (PE&F)





Privacy Impact Assessment for the Integrated Plant Health Information System (IPHIS)

January 28, 2020

Contact Point
Camille Chapman
APHIS/MRP IT
301-851-2246

Reviewing Official
Tonya Woods
APHIS Privacy Act Officer
United States Department of Agriculture
(301) 851-4076

Abstract

The system name is the Integrated Plant Health Information System (IPHIS). IPHIS provides a Web-based plant health data management system for use by all levels of plant health personnel within the Agency (e.g., executives, managers, and field personnel), as well as cooperators outside the Agency (e.g., diagnostic laboratories, state and local governments, and academia). This document has been completed in accordance with the requirements of the E-Government Act of 2002.

Overview

IPHIS is a Plant Protection and Quarantine Investment in the Animal and Plant Health Inspection Service portfolio. IPHIS provides users with an electronic interface to access, enter, and view data for plant health events nationwide. The following data is contained and provided to IPHIS users: results of plant pest, noxious weed, and biocontrol surveys to include: survey locations, target pests, survey sample identification, and diagnostic test results; survey supply orders and inventory management; domestic emergency action notifications; and compliance agreements and inspections. Any information sharing conducted by the program or system Information shared may include but is not limited to pest name, absence or presence, crop/host, location and environment in which a crop/host is found or surveyed, survey methods, and frequency and scope of a survey. IPHIS was granted an Authority to Operate by the Office of the Chief Information Officer, Cyber Policy and Oversight (CPO) on April 18, 2020.

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?

Plant pest, noxious weed, and biocontrol survey data including pest/weed names, source of data, specific crop/host, location and environment in which a crop/host is found or surveyed, survey method (visual or survey device), survey location, pest absence/presence, plant health events, diagnostic results including sample ID and confirmation method, survey supply orders and inventory management, regulatory action notifications, and tracking and control documentation. The system also collects information related to business entities and individuals such as name, address, telephone number, fax number and Longitude/Latitude.

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

Data is derived from the following sources: USDA APHIS PPQ field specialists, identifiers, and other personnel and their supervisors, other Federal Agencies, State and local government Agencies, individuals, and University cooperators.

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

The information is collected, used, disseminated, or maintained for the purpose of preparing, monitoring, and responding to plant health related issues in order to protect American agriculture. This is accomplished by: the early detection and tracking of exotic and invasive plant pests and noxious weeds to prevent spread; facilitating the export and interstate movement of agricultural products by monitoring the occurrence and distribution of certain organisms; issuing compliance agreements for the interstate movement of regulated articles; facilitating pest management by monitoring the occurrence and distribution of pests and beneficial organisms; communicating the activities and results of survey detection to cooperators and/or users on a timely basis; responding to plant health pest outbreaks; validating pest risk models; and forecasting surveys supply needs.

1.4 How is the information collected?

Information is collected by use of paper/excel spreadsheet template, and pencil/pen, or in electronic (i.e. PDA's, tablets, iPads, etc.) formatted by APHIS and/or its cooperators.

1.5 How will the information be checked for accuracy?

Automated referential integrity checks and business rules will be performed on the data as it is collected from the various identified sources. Additional referential integrity checks and business rules will be performed on the data before committing the data to the IPHIS database. Periodic manual data currency reviews will be performed by IPHIS subject matter experts to ensure data accuracy.

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

Plant Protection Act 7 U.S.C. 7701-7786; The Honey Bee Act 7 U.S.C. 281-286; Bioterrorism Preparedness and Response Act of 2002 7 U.S.C. 8401; The Food Conservation and Energy Act 2008 7 U.S.C. 8791; Compliance Agreements; Emergency Action Notifications; and scientific survey methodology.

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

The privacy risks identified would be integrity and availability of the data. The risks are mitigated thru the use of 2-layer authentication. Integrated Network Authentication is required for access to the system. The role based access control list for the database validates against the network identification of the user creating a 2-layer authentication schema. This controls who has access to the system.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The principle use of the information is for preparation, monitoring and response to plant health related issues. The data will describe pest status and location to plant health responders, senior level federal and state policy makers. Specifically, the information will be used as an information tool to help determine what effective action must be taken when a plant pest or noxious weed is found. Additional uses of the information will be to facilitate the export and interstate movement of agricultural products; the issuance of compliance agreements for the interstate movement of regulated articles; to facilitate management of pests and beneficial organisms; to communicate the activities and results of survey detection to users on a timely basis; to monitor the distribution of pests; to respond to a plant health pest outbreak; to forecast survey supply needs; and to validate pest risk models. COGNOS extracts Plant pest, noxious weed, and bio-control survey data to generate reports that are used for Data analysis and program management decisions. County level summary data will be exported from IPHIS then uploaded into the National Agricultural Pest Information System (NAPIS), Purdue University, to support the web based public interface site Pest Tracker for the Cooperative Agricultural Pest Survey Program.

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

The system uses COGNOS business intelligence software for generating reports regarding plant health data within the system.

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

ESRI provides the street map and aerial photography that serve as a background/reference maps for the display of IPHIS data. ESRI also provides geographic coordinates when a location address is entered but the latitude and longitude data are missing. Open Street maps are used on the iOS Mobile data collector for mapping on the mobile devices.

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.

Role based robust authentication and authorization via USDA eAuthentication; physical access control, firewalls (access control), intrusion detection systems, and system auditing are among the countermeasures used to prevent unauthorized access. Additionally, all cooperators authorized to access information have signed a General Memorandum of Understanding in which they have agreed to safeguard the confidentiality of such data and prohibit unauthorized access to the data provided by USDA APHIS. They also agree not to release any of the data provided by USDA APHIS, and to refer any and all requests for the data provided to USDA APHIS Legislative and Public Affairs, Freedom of Information and Privacy Act Office.

Section 3.0 Retention

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

3.1 How long is information retained?

The data is to be retained in the database permanently.

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

A retention period has not been formally established for data at this time. We are working with the APHIS records management officer to establish a data retention schedule.

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

No risks have been identified with the length of time for retention of the data.

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?

Information shared may include but is not limited to pest name, absence or presence, crop/host, location and environment in which a crop/host is found or surveyed, survey methods, and frequency and scope of a survey. USDA APHIS, and sister agencies such as Agricultural Research Service, Forest Service, National Institute of Food and Agriculture, Natural Resources Conservation Services, Risk Management Association, and Farm Service Agency may use this information for pathway analysis, trade, risk analysis, science, and any other uses necessary to support or to enhance USDA program goals.

4.2 How is the information transmitted or disclosed?

Information deemed necessary to share may be transmitted or disclosed by verbal communication, paper, or electronic means.

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.

The system has built in granularity based on the level of access deemed appropriate by IPHIS Business System Manager and System owner. This level of access is based on individual needs without compromising the integrity or security of the data. Additionally, when any personally identifiable data is shared all personnel are advised of the rights provided individuals, agricultural producers, or owners of agricultural lands under the Privacy Act of 1974, the Freedom of Information Act, and The Food Conservation and Energy Act 2008 7 U.S.C. 8791.

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?

Information may be shared with cooperators from state and local governments, plant health officials, cooperators from academic institutions, and diagnostic laboratories. Information to be shared may include but is not limited to pest name, absence or presence, location, host, survey methods, and frequency and scope of pest survey.

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.

Yes, personally identifiable information is being shared. A SORN is being developed at this time. This deficiency has been noted in POA&M number 28367. The personally identifiable information is being shared under the guidelines and authorities of the Plant Protection Act 7 U.S.C. 7701 et seq., and the Food Conservation and Energy Act of 2008 7 U.S.C. 8791. All cooperators that information is shared or exchange with have signed a General Memorandum of Understanding in which they have agreed to safeguard the confidentiality of such data and prohibit unauthorized access to the data provided by USDA APHIS. They also agree not to release any of the data provided by USDA APHIS, and to refer any and all requests for the data provided to USDA APHIS Legislative and Public Affairs, Freedom of Information and Privacy Act Office.

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

Information may be shared by electronic means, verbally, and in paper format, and is determined by secure role based data access. Any personally identifiable information shared is done under the guidelines and authorities of the Plant Protection Act 7 U.S.C. 7701 et seq., and the Food Conservation and Energy Act of 2008 7 U.S.C. 8791. All cooperators/collaborators that information is shared or exchange with have signed a General Memorandum of Understanding in which they have agreed to safeguard the confidentiality of such data and prohibit unauthorized access to the data provided by USDA APHIS. They also agree not to release any of the data provided by



USDA APHIS, and to refer any and all requests for the data provided to USDA APHIS Legislative and Public Affairs, Freedom of Information and Privacy Act Office.

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

The privacy risks identified are the further disclosure of 1) information pertaining to specific locations and environment in which a crop/host is found or surveyed, and 2) points of contact and information provided by an agricultural producer or owner of agricultural land, concerning the agricultural operation, farming or conservation practice, or of the land itself. Personally identifiable information is shared by following the guidelines and authorities of the Plant Protection Act 7 U.S.C. 7701 et seq.; The Honey Bee Act 7 U.S.C. 281-286; and the Food Conservation and Energy Act of 2008 7 U.S.C. 8791. Additionally, all cooperators/collaborators that information is shared or exchange with have signed a General Memorandum of Understanding in which they have agreed to safeguard the confidentiality of such data and prohibit unauthorized access to the data provided by USDA APHIS. They also agree not to release any of the data provided by USDA APHIS, and to refer any and all requests for the data provided to USDA APHIS Legislative and Public Affairs, Freedom of Information and Privacy Act Office.

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, and a SORN is being developed at this time. This deficiency has been noted in POA&M number 28367

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?

No, if they consent to provide info.

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.

Notification is either verbally from USDA personnel in official uniform or by written notification in the form of flyers or written notices left at the property to be surveyed. There is no risk because individual are always notified.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Any individual may obtain information from a record in the system that pertains to him or her. Requests for hard copies of records should be in writing, and the request must contain the requesting individual’s name, address, name of the system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager at the address above. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

Publication of the Systems of Records Notification (SORN) provides information on access and amending information collected in IPHIS. The agency also provides the public with information via publically accessible websites. For example the FOIA Reading Room can be accessed at the following web address:

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

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 are no privacy risks because redress is done according to guidelines set forth by the Freedom of Information and Privacy Act Staff.

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?

Role based access controls and personnel security policies will be implemented and followed as part of the baseline security requirements. Moreover, a position sensitivity matrix will be developed and continually maintained to determine whether access is required and the appropriate level of access if it is deemed necessary.

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?

All APHIS personnel and contractors are required to complete the Computer Security and Accessibility test annually.

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

Accreditation and Authority to Operate was awarded on April 18, 2018.

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

Robust authentication and authorization via USDA eAuth, physical access control, firewalls (access control), intrusion detection systems and system auditing are among the countermeasures used to prevent unauthorized access and misuse of data.

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?

The privacy risks identified are the further disclosure of information pertaining to specific locations and environment in which a crop/host is found or surveyed, and points of contact and the information provided by an agricultural producer or owner of agricultural land, concerning the agricultural operation, farming or conservation practices, or of the land itself. Personally identifiable information is shared by following the guidelines and authorities of the Plant Protection Act 7 U.S.C. 7701 et seq.; The Honey Bee Act 7 U.S.C. 281-286; and the Food Conservation and Energy Act of 2008 7 U.S.C. 8791. Additionally, all cooperators/collaborators that information is shared or exchange with have signed a General Memorandum of Understanding in which they have agreed to safeguard the confidentiality of such data and prohibit unauthorized access to the data provided by USDA APHIS. They also agree not to release any of the data provided by USDA APHIS, and to refer any and all requests for the data provided to USDA APHIS Legislative and Public Affairs, Freedom of Information and Privacy Act Office.

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?

Web-based plant health data management system with mobile data collectors.

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

The project does not employ any technology that would raise privacy concerns.

Section 10.0 Third Party Websites/Applications

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

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

Yes.

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

The 3rd party website is used to provide Mapping service data such as Base maps, which provides world topography, street demographic, and reference overlay information that is available in public domain
<https://unpkg.com/leaflet@2.1.3/dist/leaflet.js>

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

No PII data would become available as a result of the use of 3rd party website.



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

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?

No



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?

System does not use web measurement or customization technology

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency’s use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A

Responsible Officials

Camille Chapman
United States Department of Agriculture

Approval Signature

Preston J. Griffin
Acting Chief Information Security Officer (CISO)
Marketing and Regulatory Program IT
United States Department of Agriculture

Tonya G. Woods
Privacy Act Officer
Animal and Plant Health Inspection Service
United States Department of Agriculture

William M. Newton
IPHIS System Owner
Animal and Plant Health Inspection Service
United States Department of Agriculture