

Privacy Impact Assessment APHIS ServiceNow System

Technology, Planning, Architecture, & E-Government

- Version: 1.1
- Date: September 11, 2015



Privacy Impact Assessment for the APHIS ServiceNow System

September 11, 2015

Contact Point

Cynthia A. MacLeod-Sims
Animal and Plant Health Inspection Service
301 851-3033

Reviewing Official

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

Danna Mingo, APHIS Privacy Liaison
United States Department of Agriculture
(301) 851-2487

Chief Privacy Office
Office of Chief Information Office
United States Department of Agriculture

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Animal and Plant Health Inspection ServiceNow System. The ServiceNow Software as a Service (SaaS) provides information Technology Service Management (ITSM) capabilities. The PIA was conducted because the ServiceNow SaaS has the potential to store personally identifiable information within the cloud provided solution.

Overview

The Animal and Plant health Inspection Services (APHIS) of the United States Department of Agriculture (USDA) is charged with protecting the health and value of American agriculture and natural resources from the introduction of destructive plant and animal diseases and pests. These efforts support the overall mission to protect and promote agriculture and natural resources. The purpose of the ServiceNow SaaS is to provide complete ITSM capabilities to federal and non-federal employees working to fulfill the mission of inspecting protecting animal and plant materials within the United States.

Organizationally Marketing and Regulatory Programs Business Services (MRPBS) is located with APHIS, which is the lead agency in providing administrative support for MRP. MRPBS has several divisions which address a variety of employee and customer needs, to provide administrative support services in the area of budget, finance, human resources, information technology, procurement, property management, and related administrative services.

This PIA is being created for the APHIS ServiceNow instance which is a cloud provided solution.

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?

APHIS ServiceNow collects name, email address, contact numbers, general location (ie State or Intl) and if the data is coming from a Government employee or someone from the general public in order to get IT service.

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

The source of the information is the USDA/APHIS employees, contractors and general public who call in to the APHIS helpdesk.

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

The data is being collected in order to provide helpdesk service to the customer. The information may be used to create reports and other files related to customer query and problem response; query monitoring; and customer feedback records; and related trend analysis and reporting.

1.4 How is the information collected?

The information is emailed or provided over the phone to the helpdesk personnel.

1.5 How will the information be checked for accuracy?

When data is provided via email the data is entered into the Service Desk solution as provided by the customer and is not check for accuracy.

When the data is provided over the phone the only validation of the data happens when the information about the customer's contact information is automatically pulled directly from Active Directory when the correct customer is selected in the search box.

For e-Authentication (eAuth) related system access and transactions, eAuth does this externally.

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

- a. The Animal Welfare Act
- b. The Plant Protection Act
- c. The Animal Health Protection Act
- d. The Virus-Serum-Toxin Act

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

Unauthorized disclosure of employee and other personal data, as identified in Section 1.3 above, was the primary privacy risk. Privacy rights of the employees and external

parties/persons will be protected by USDA, APHIS and MRPBS management by the following means:

- All access to the data in the system is controlled by formal authorization. Each individual's supervisor must identify (authorize) what functional roles that individual needs in the APHIS ServiceNow instance.
- All access to the system is controlled by the USDA Active Directory authentication and the APHIS VPN. No action can be performed without first authenticating into the system.
- Application limits access to relevant information by assigned application functions to roles. This prevents access to unauthorized information.
- The USDA warning banner must be acknowledged at application login.

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 information is only used as contact information in order to provide service to the customer.

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

N/A – no special tools in use

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

Not Applicable

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.

The APHIS ServiceNow instance is protected through the use of eAuth/ADFS and LincPass

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?

APHIS is proposing to retain information/records Items are retained per the General Records Schedule (GRS) 24: Information Technology Operation and Management Records with one set of records following a newly established schedule. Records are destroyed based on the subject matter. <http://www.archives.gov/records-mgmt/grs/grs24.html>

The data is retained as per specified for system backup and tape libraries. Data is backed up as a monthly full backup, with daily incremental backups, and then superseded by the next full backup. Data is retained for 3 years Some of the identified records include, but are not limited to, system back-ups; user and customer identification, profiles, authorizations, etc.; knowledge articles and frequently asked questions; help desk logs and reports; and other records pertaining to customer query and problem response, query monitoring and clearance, customer feedback, and related trend analysis and reporting. The retention of these records vary.

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

The scheduling of the records retention schedule has not been approved by NARA. The request has been submitted and 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.

The data in the system is used for administrative purposes. The PII collected is minimum and no risk had been identified related to the use 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?

Not Applicable

4.2 How is the information transmitted or disclosed?

Not Applicable

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.

Not Applicable.

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?

Not Applicable: No data is shared outside of the USDA

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.

Not Applicable.

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

Not Applicable

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

Not Applicable

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?

There is no notification provided to the individual prior to the collection of the information because the potentially PII data, if any, is provided on a voluntary basis by the callers to the helpdesk.

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

Yes, providing personal information is at the discretion of the customer leaving contact information.

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

Yes, users have the right to provide or not provide required information. If the individual refuses use then the system will not continue processing the user's request.

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.

All users who access the APHIS ServiceNow application, are presented with the standard USDA warning banner that must be acknowledged prior to logging into the system.

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?

Through the APHIS ServiceNow Self-Service Portal, customers can see part of their profile and could notify us of changes. APHIS employees can update their information through the Address Book Tool which updates EAD & those changes would be pushed down to their APHIS ServiceNow profile.

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

The customer is contacted to correct the email address. Phone numbers are verified whenever a customer calls in. The data is checked for accuracy by the customer when entering ticket information into the service desk solution. Information about the customer's contact information is automatically pulled directly from Active Directory when the correct customer is selected in the search box. For eAuthentication related system access and transactions, eAuth does this externally, and is not part of the AEI boundary

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

Not Applicable

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

See 7.1 comment

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 no identified risk associated with the redress

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?

APHIS implements a Rules of Behavior (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the USDA implementation of User Security Awareness training which is provided annually by the Department.

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?

APHIS Marketing and Regulatory Programs Business Services (MRPBS), under the information Systems Security Manager (ISSM) staff administers and tracks APHIS Security & Privacy training. Training is required annually and the records are maintained as part of office documentation for employees and contractors.

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

No, the A&A is in progress at the time of the submission of this document.

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

All users are required to have an individual user account to the application system

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?

Not Applicable

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?

The APHIS ServiceNow instance is a software-as-a-service offering (managed, hosted service) that includes all required hardware, network, software, user administration, system / application monitoring, maintenance / administration and other required management activities to automate the following IT enterprise support functions:

- Change management ;

- Release & Deployment Management;
- Service desk (incident management) ;
- Problem management ;
- Knowledge management ;
- Service request and service catalog and
- Service Asset & Configuration Management

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

The system does not utilize any technologies that would raise the Privacy Risk.

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?

Office of Management and Budget memorandum M-12-10

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

Not Applicable

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

Not Applicable

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

Not Applicable

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

Not Applicable

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

Not Applicable

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

Not Applicable

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

Not Applicable

10.10 Does the system use web measurement and customization technology?

Not Applicable

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

Not Applicable

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

Not Applicable

Please note that records within the ServiceNow may be retrieved by a personal identifier such as a name however, it is only for administrative purposes to provide IT service to the customer. There is no evidence that the names of contact persons will be used to obtain information about that person. The agency has determined that the risk impact and privacy impact of this data retrieval is very low therefore a SORN is not required. This decision is supported by the *Henke vs US Department of Commerce* 83 F.3d 1453 (D.C. Circuit 1996) page 24 of the Overview of The Privacy Act 2010 Edition.



Approval Signature

Cynthia A. MacLeod-Sims
System Owner – APHIS ServiceNow
Animal and Plant Health Inspection Service
United States Department of Agriculture

Rajiv Sharma
APHIS Information System Security Program Manager
Animal and Plant Health Inspection Service
United States Department of Agriculture

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