Privacy Impact Assessment
APHIS ServiceNow System

Policy, E-Government and Fair Information Practices

- Template Version: 1.4
- Date: May 15, 2023
- Prepared for: Marketing and Regulatory Programs

USDA
United States Department
of Agriculture

Privacy Impact Assessment for the

APHIS ServiceNow System

May 15, 2023

Contact Point

Michael Brandon Peach
Animal and Plant Health Inspection Service
(919) 855-7139

Reviewing Official

Angela Cole
Assistant Chief Information Security Officer/Chief Privacy Officer
United States Department of Agriculture

Abstract

The United States Department of Agriculture (USDA) Animal and Plant Health Inspection Services (APHIS) uses ServiceNow to support the end-to-end delivery of IT services. ServiceNow is a vendor-supported Platform-as-a-Service (PaaS) that provides Information Technology Service Management (ITSM) capabilities. USDA APHIS is republishing this Privacy Impact Assessment (PIA) to discuss the personally identifiable information (PII) collected and processed within the APHIS ServiceNow platform, as well as analyze the privacy risks.

Overview

The Marketing and Regulatory Programs (MRP) is a mission area within USDA that facilitates domestic and international marketing of U.S. agricultural products, protects U.S. plant and animal health, regulates genetically engineered organisms, administers the Animal Welfare Act, and carries out wildlife damage management activities. MRP agencies are active participants in setting national and international standards. The two main programs under MRP include: Agricultural Marketing Service (AMS) and Animal and Plant Health Inspection Service (APHIS). To support its mission, APHIS leverages information technology (IT) to support its operations for employees, contractors, and customers.

The Marketing and Regulatory Programs Business Services (MRPBS) is located within APHIS, which is the lead agency in providing administrative support for Marketing and Regulatory Programs (MRP). MRPBS has several divisions which address a variety of personnel and customer needs, to include information technology, procurement, emergency incident management, property management, and related administrative services.

MRPBS IT supports IT services for APHIS Program Offices to excel in its mission. APHIS ServiceNow is a system managed by the MRP IT to support and manage IT service requests. This PIA is exclusively focused on the APHIS ServiceNow tool, which processes IT service requests for APHIS personnel and contractors, as well as its external customers. In addition, APHIS' ServiceNow manages project suggestions and proposals for the Plant Pest and Disease Management and Disaster Prevention Program under the Plant Protection Act Section 7721 (PPA7721).

APHIS ServiceNow

The APHIS ServiceNow is a robust ITSM tool that supports MRPBS IT enterprise support functions. ITSM process assists USDA to manage IT services to both internal and external users. APHIS ServiceNow includes the following modules to support its IT operations:

- **Service Request & Service Catalog** is the process of cataloging services to support operations and fulfillment of MRP processes.

- **Change Management** to manage, track or configuration changes within IT configuration. IT Configuration release to a new system, Implementation of a device or a change to business service.
- **Release & Deployment Management** to addresses changes and improvements to existing services within MRP IT environment.
- **Service Desk** includes the practice of resolving customer issues or restoring services to MRP-IT products.
- **Problem management** to resolves large scale issues for MRP-IT products.
- **Knowledge Management** includes the collection of documentation, policies and procedures for various MRP mission area.
- **PPA7721** supports pest detection, surveillance and identification, threat mitigation, and safeguarding the nursery production system and responding to plant pest emergencies.

Service Request Management

A central component to the ITSM process is service request management. The MRP IT teams receive a wide variety of service requests from APHIS personnel and external customers. This uniquely involves an individual request technical assistance for applications, software licenses, password resets, or new hardware (e.g., laptop, printer, phone). MRPBS IT is dedicated to responding to and fulfilling requests and uses APHIS ServiceNow to automate the lifecycle of service requests from intake to resolution.

APHIS ServiceNow allows APHIS personnel (referred to as *internal users*), and external customer users (referred to as *external users*) to submit service requests for technical assistance. Internal users may initiate a service request ticket through the self-service portal, or by contacting the Service Desk by phone or email. There is also a live chat feature for instant communication with internal users. External users access a separate portal designed to support customer service needs. External users may also call report and resolve issues.

The creation of the service ticket includes the collection of limited contact information from the user. The degree of information collected varies depending on the service request type. The types of service request supported by ServiceNow includes, but is not limited to:

- Web Domain Request
- Telework and Remote Work Agreement
- Application Support Requests
- Building Access Request
- Telecom Request
- New Incident
- System and Data Access Request

- Microsoft Teams Request
- Reset Password

At a minimum, service request tickets collect the requestor's name and contact information. This information is used to identify and communicate with the user about their service request. APHIS ServiceNow generates a ticket with a unique ticket number once a service request is completed. Once the Service Desk ticket is created, it is assigned to the appropriate IT representative for resolution. All tickets are instantaneously processed and may be immediately accessed by the requestors who submitted the initial service request via the portal or email message.

All service requests are triaged to MRPBS IT for assignment and resolution. IT representatives investigate service requests and use APHIS ServiceNow to include working notes about the ticket. MRP IT updates the system once the ticket is closed and completed. APHIS ServiceNow emails both internal and external users with a brief explanation of the issue and resolution, as well a survey. This survey is voluntary and helps MRP improve its service operations. No additional PII is collected from the users. The survey results are associated with the user and is linked to the ticket number. Closed tickets are archived but remains in APHIS ServiceNow for trend analysis and reporting.

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?

Information collected from USDA internal users include:

- Full name [first, middle initial, last]
- Title
- Program Unit
- Work Location
- Telephone number [i.e., work, home or mobile]
- Email address
- Supervisor Name
- Supervisor Email
- Attachments
- Request type
- Survey feedback

Information collected from USDA external users include:

- Full Name
- Mailing address
- Telephone address [i.e., work, home or mobile]
- Photographic images
- Request type
- Survey feedback

Information collected under the authority of PPA7721 include:

- Full Name
- Mailing address
- Phone Number

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

APHIS ServiceNow collects information directly from USDA internal users and external costumer users. USDA personnel data is also derived from USDA Enterprise Active Directory (EAD) and USDA eAuthentication.

MRPBS Human Resource Division (HRD) provides employee information to support HR operations associated with Telework and Remote Work Agreement support.

PPA7721 collects and approves information from project suggestions submitted by internal and external users of the application.

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

APHIS ServiceNow allows individuals to request IT support, report problems, order equipment and software, and check the status of inquiries. Information collected from USDA employees and external users is collected provide technical assistance incoming queries and issues related to computer systems, software, and hardware. The information is used to create a service ticket, contact customers, create reports and other files to resolve the issue. Information many also be used to for customer feedback and trend analysis and reporting.

APHIS ServiceNow also collects data for the Plant Protection Act, PPA7721. APHIS' ServiceNow manages project suggestions and proposals for Plant Pest and Disease Management and Disaster Prevention Program. APHIS annually makes funds available to state government, universities, nonprofit institutions, industry and tribal nation cooperators, to support projects that protect specialty crops, other agricultural production, nursey systems, forestry and other natural resources from harmful and exotic plant pest and pathogens.

Employee HR information is provided by MRPBS HRD for the purposes of informing employees of their own HR information related to their established Telework or Remote Work Agreement status and to enable auditing by MRPBS HRD staff supporting employees for these agreements.

1.4 How is the information collected?

Data is collected directly from all users who make service or incident request. Data collected from email and telephone requests are manually entered into APHIS ServiceNow by IT Support. For individuals who call into the Service Desk, the IT representative asks a series of questions to confirm the caller's identity and intake the service request. USCIS ServiceNow automates and prepopulates the internal user's full name using EAD or eAuthentication.

External users are verified via eAuthentication and cannot be verified using EAD. Information is collected directly from the individual self-service portal or by the IT Support representative who enters information into the service request form. APHIS ensures data accuracy in APSIC ServiceNow through program coding to mitigate or prevent inconsistencies in data.

External users who submit information for PPA7721 access the system via a level 1 or 2 USDA eAuthentication.

HR employee information is collected by MRPBS HRD and delivered for import into the MRP ServiceNow Platform.

1.5 How will the information be checked for accuracy?

APHIS and AMS affiliated data is validated against EAD and eAuthentication automatically each time a user logs into the system. Manual verification for non-APHIS or AMS affiliated is performed by Support Staff providing support when a user calls in or an issue is discovered. When data is provided via email the data is entered into the Service Desk solution as provided by the customer and is not checked 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.

MRPBS HRD provided employee information is validated by HRD staff prior to delivery for load into the MRP/APHIS ServiceNow platform.

Information collected under PPA7721 is reviewed for accuracy by Plant Protection and Quarantine staff once the open period for project submission is closed. The list of reviewers (who have eAuth access) will go in the system and review submission and assess the accuracy of the submitted information.

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

APHIS ServiceNow application has been established to support MRP-IT . Authority to conduct these processes are supported in the following legal authorities:

a. It is required under Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Guidance can be found in Appendix III to OMB Circular No. A-130 and NIST SP 800-30, *Risk Management Guide for Information Technology Systems.*

b. E-Government Act of 2002 (H.R. 2458/Pub. L. 107-347); Public Law 107-347

c. OMB Circular A-130: Managing Information as a Strategic Resource

d. OMB Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities

e. OMB M-11-29

f. Homeland Security Presidential Directive 12 (HSPD-12)

g. Plant Protection Act (Title IV, Pub.L. 106-224, 114 stat.428.7 U.S.C. 7701-7721)

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

There is a privacy risk that APHIS ServiceNow may collect more information than necessary to support ITSM processes. Limited PII about USDA internal and external users are collected to create a service ticket. Only the minimum amount of contact information and data about the issue are collected and used to resolve the issue. Internal users may upload files associated with the requests for service and support. These files may include PII and other business sensitive information. Due to technical limitations, there are limited restrictions placed on the types of files that may be uploaded, or the content they may contain. As such, it may be possible for files that contain sensitive PII or business sensitive information. This risk is partially mitigated as the system maintains the appropriate technical controls to secure the information from unauthorized access and disclosure.

An additional privacy risk is the unauthorized access and disclosure of PII. All records in APHIS ServiceNow is protected by APHIS and MRPBS management by the following means:

- Designated technician to have access to the data in the system, which 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 eAuth. 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 eAuth warning banner must be acknowledged at application login.
- Regular auditing of access to ensure only authorized individuals have 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.

APHIS uses the information within APHIS ServiceNow to:

- Intake service and incident requests
- Triage and assign tickets to appropriate IT and program support personnel
- Contact customers to provide important notification and status updates
- Create reports and other files related to customer query and problem response
- Query monitoring
- User customer feedback to enhance the system and ITSM process and related trend analysis and reporting.
- Project suggestions for Plant Pest and Disease Management and Disaster Prevention.
- Proposals for Plant Pest and Disease Management and Disaster Prevention.
- Authorizes funding for Plant Protection and Quarantine programs.
- Provide HR Telework and Remote Work related support to MRP employees

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

Not Applicable – no special tools are used.

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 eAuthorization. Access to data in the system is controlled by user roles which are assigned appropriately to the end users with permission to view and edit data based on role. User approval and removal requirements are provided by the system owner.

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 ServiceNow records are covered under the following National Archives and Records Administration (NARA) General Record Schedule (GRS):

- GRS 3.1 destroy 5 year after system is superseded by a new iteration, or is terminated, defunded or no longer needed.[1]
- GRS 4.1 destroy no sooner than 6 years after the project or activity or transaction is completed.[2]
- GRS 5.8 destroy 1 year after resolved or when no longer needed for business use.[3]
- Records for PPA7721 will be maintained indefinitely until a records schedule is created and approved by NARA.

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

Yes. APHIS ServiceNow records are governed under the NARA GRS 3.1, 4.1 and 5.8. A separate APHIS ServiceNow records schedule is not required.

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

[1] grs03-1.pdf (archives.gov)
[2] grs04-1.pdf (archives.gov)
[3] grs05-8.pdf (archives.gov)

There is an inherent risk that PII is retained longer than necessary to fulfill specified purposes. NARA issues GRS to provide disposition authority for records common to several or all agencies of the Federal Government. These schedules authorize agencies, after specified periods of time to destroy temporary records.. USDA adheres to the GRS issued by NARA, which is the agency that oversees the scheduling of records. The NARA GRS applicable to APHIS ServiceNow is consistent with the concept of retaining data only for as long as necessary to support its core functions. Help desk services are provided to USDA government and contract employees' technical and administrative questions. These schedules cover records on managing administrative technical and IT help desks.

There is no additional risk associated with the indefinite length of time data is retained for PPA7721. Until a records schedule is approved, data is permanent and encrypted. Once a schedule is approved, data will be maintained and disposed of in accordance with APHIS records retention schedules (except where litigation and other holds apply), access control procedures, and APHIS Directive 3440.2, which outlines the appropriate procedures for disposing of media and data on media in a manner that makes it impossible to recover.

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. APHIS does not share APHIS ServiceNow information with internal entities. Nor is information from PPA7721 shared with internal entities.

4.2 How is the information transmitted or disclosed?

Not Applicable. APHIS does not share APHIS ServiceNow information with internal entities.

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.

There is no privacy impact related to external information sharing because information from APHIS ServiceNow is not shared with external entities.

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. APHIS does not share APHIS ServiceNow information with external entities.

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. No data from APHIS ServiceNow is shared outside of USDA.

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

Not Applicable. No data from APHIS ServiceNow is shared outside of USDA.

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

Not Applicable. There is no privacy impact related to external information sharing because information from APHIS ServiceNow is not shared with external entities.

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.

A SORN is required and is in the creation process.

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

APHIS provides notice to individuals prior to accessing system and the collection of information. On the logon page, individuals are required to read and acknowledge a logon warning banner that describes the conditions of use and access, as well system monitoring. Once logged on, the ServiceNow homepage includes a Privacy Notice . The Privacy Notice informs the individual about the authority to collect the information requested, purposes for collecting it, routine uses, and consequences of providing or declining to provide the information to APHIS. Additionally, the general public receives general notice through the publication of this PIA.

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

Yes, both internal and external users voluntarily share their data to obtain IT support and users can choose whether to provide this information. However, if a customer refuses to provide required information, MRPBS IT cannot provide IT support.

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

Yes, the logon warning banner collects express consent from the individual that information collected and stored this information system may be used for monitoring purposes. Individuals who do not consent to system monitoring are not provided access to the system.

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.

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?

Individuals may report a technical issue and create a service request ticket in APHIS by phone, online webform, and chat. Individuals who call to report a service request receive a system-generated email detailing the issue and status of the request. The external-facing portal allows internal and external users to electronically engage with MRP

ServiceNow Administrators as well as view submitted tickets, as well as their profile data.

External user’s associated that submit information under PPA7721 have eAuth access and can self-correct inaccurate or erroneous information of the information that they submitted.

Additionally, individuals may seek access to his or her APHIS records by filing a Privacy Act or Freedom of Information (FOIA) request. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Any person may file a FOIA request. USDA offers several avenues to request access to their records. Individuals may file a Privacy Act or FOIA request to view their record by submitting a FOIA request online through USDA’s Public Access Link (PAL), or through mail or fax.[4]

USDA – Animal and Plant Health Inspection Service
FOIA/PA Director
4700 River Road, Unit 50
Riverdale, MD 20737
Facsimile: 301-734-5941
Email: APHISPrivacy@usda.gov

Further information about Privacy Act and FOIA requests for APHIS records is available at https://www.aphis.usda.gov/aphis/resources/foia.

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

USDA MRP APHIS offers multiple opportunities for individuals to correct inaccurate or erroneous information. Individuals may use the self-service portal on the ServiceNow platform (https://help.aphis.usda.gov/sp) and contact the Technical Assistance Center support or submit a request to the FOIA/Privacy Officer. Each user is assigned an online account and are offered self-services tools to manage the data stored in their account. 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. Individuals are able to review and edit their data at any time. If incorrect information is presented to the user via the call center or online form, individuals may correct their information in real-time. For example phone numbers are verified whenever a customer calls in, and individuals may edit data when entering ticket information into the online form.

[4] https://efoia-pal.usda.gov/App/Home.aspx

User's associated with PPA7721 have eAuthentication access and can self-correct inaccurate or erroneous information of the information that they submitted via USDA eAuthentication Self-Service Portal (www.eauth.usda.gov). Project information that requires update or correction can resubmit the project via PPA7721 self-service portal (https://help.aphis.usda.gov/ppa7721) prior to the end of the current submission open season or contact Plant Protection and Quarantine staff supporting PPA7721.

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

The APHIS website, the APHIS ServiceNow portal, the Help Desk, and this PIA explains how an individual may correct his or her information once obtained by APHIS ServiceNow. Specific instructions for both USDA personnel and external users are posted within the portal. External users receive automated notifications that provide contact information for the APHIS Helpdesk should they need to correct their information or obtain any additional support.

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

Not applicable as formal redress is offered to both USDA personnel and external users.

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 minimal privacy risk related to redress. USDA provides individuals with access, amendment, or correction to their records through multiple avenues.

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?

All APHIS employees and contractors are provided access to submit a service request for technical assistance. Any APHIS employee with appropriate credentials to access the USDA APHIS network may gain access to ServiceNow.

Access to the back-end system is limited to IT support representatives to track and manage service requests. Access to the system is controlled by user roles which are assigned appropriately to end users with permissions to view and edit data based on role. The APHIS ServiceNow system owner determines access and roles for users. Access to the system is documented in the system user guide and standard operating procedures. The user access list is reviewed several times a year by the system owner.

All users who require access to PPA7721 within ServiceNow must have USDA eAuthentication level 2 access to the system. Users requesting access to submit project suggestions will contact APHIS Plant Protection and Quarantine for access to PPA7721.

8.2 Will Department contractors have access to the system?

Yes. Contractors supporting APHIS have access as general users and IT support staff.

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

All users of APHIS ServiceNow including contractors are required to complete annual USDA Information Security awareness training which includes privacy. Successful completion of the training is required prior to being granted access and annually thereafter in order to maintain access.

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

Yes. The APHIS ServiceNow system was granted an Authority to Operate (ATO) on May 10, 2021 and expires on May 10, 2024. ServiceNow also received a FedRamp ATO for a high system.[5]

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

All information is secured through appropriate technical controls to prevent the misuse of data. All users are required to have an individual user account (Level 2 eAuth Account) as well as a user account within APHIS ServiceNow to access the system. Each user is granted specific access privileges based the need-to-know. Defined user roles and record access controls provide appropriate access to data. Users are prohibited from allowing others to use their account and from accessing other users' accounts. Users are individually accountable for all actions under their logon credentials through signed Rules of Behavior.

APHIS ServiceNow is hosted on a federal government ServiceNow platform that includes enhanced encryption and data monitoring and can only be access through USDA LAN and VPN. The use of APHIS ServiceNow requires the acknowledgement and consent to monitoring and auditing of the system. Monitoring includes the tracking

[5] FedRAMP was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services to federal agencies, and to accelerate the adoption of secure cloud solutions by federal agencies.

of transactions within USDA networks and external transactions. Both internal and external users are appropriately informed that there is not expectation of privacy when using or storing data on government information systems. Administrators regularly audit access.

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 are minimal risks to privacy. USDA APHIS ServiceNow has appropriate technical controls to securely maintain the data.

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?

APHIS ServiceNow application is a platform as a service (PaaS). APHIS Salesforce is supported by a third-party vendor. The ServiceNow GovCommunityCloud obtained FedRAMP High Impact Provisional Authority to Operate (P-ATO) from the Joint Authorization Board. This system is authorized to store PII data with authorized levels of security controls.[6]

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

The information stored in APHIS ServiceNow is managed in a vendor managed system and may be vulnerable to breach because the security controls may not meet system security levels required by USDA. These technology risks are mitigated because USDA is responsible for all data under its control - whether on a USDA or vendor's infrastructure. Therefore, USDA requires the exact security requirements and controls on vendors for safeguarding PII data. This is validated through the FedRAMP certification and the USDA security assessment authorization process.

Section 10.0 Third Party Websites/Applications

[6] FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. More information at: https://www.fedramp.gov/

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?

APHIS ServiceNow is a third-party vendor cloud-based ITSM platform. APHIS customers may submit a service request for technical support. The platform offers a set of workflows and tools for managing IT services on behalf of APHIS. APHIS ServiceNow used to handle incidents, service requests, problems, and changes.

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

ServiceNow collects PII from internal and external users as described in Section 1.0. No additional PII is directly collected from individuals. More information on its information collection practices is described in the ServiceNow Privacy Policy.[7]

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

Information collected and maintained by APHIS ServiceNow is only used to support the IT services to APHIS.

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?

ServiceNow is a Fed-Ramp approved cloud system. APHIS ServiceNow also has a USDA-issued ATO.

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

[7] Privacy Statement | IT Service Management Software, SaaS | ServiceNow

The data adheres to the NARA GRS. The tool has the capability to set a disposition schedule.

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

ServiceNow Customer Data to provide and support the Service, including updating and maintaining the Subscription Service and providing Support and Expert Services.

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?

ServiceNow does not use, disclose, review, share, distribute, transfer, or reference any internal or external user data except as permitted in the contractual agreement or as required by law.

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)?

No.

10.10 Does the system use web measurement and customization technology?

Yes. ServiceNow embeds online tracking tools to support the functionality of the tool.[8] Google Analytics cookies are also used to track the traffic of the site.

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?

Users may disable cookies through their browser settings.

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.

There is the privacy risk that the online tracking tools collect more information than necessary to operate the ServiceNow, as well as cross-site tracking. This risk is

[8] https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0693221

minimized because no cross-tracking cookies are deployed. APHIS ServiceNow uses cookies that are strictly necessary to operate the platform. The ServiceNow cookies are required for the website to function and provide the basic information requested by the website user. Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. USDA uses Google Analytics to track website visitors and their interaction with the online portal. Only aggregated and statistical information is collected for analytical purpose purposes. AMS uses Google Analytics to create summary and aggregated statistics. This data is then used to improve the way the website works and in turn, used to improve user experience.

Responsible Officials

MICHAEL PEACH Digitally signed by MICHAEL PEACH
Date: 2023.05.16 07:44:12 -04'00'

Michael Brandon Peach,
System Owner – APHIS ServiceNow
Animal and Plant Health Inspection Service.
United States Department of Agriculture

Approval Signature

JANELLE JORDAN Digitally signed by JANELLE JORDAN
Date: 2023.05.16 09:23:34 -04'00'

Janelle Jordan
APHIS Privacy Act Officer
United States Department of Agriculture

ANGELA COLE Digitally signed by ANGELA COLE
Date: 2023.05.19 11:02:22 -04'00'

Angela Cole
MRP Chief Privacy Officer/Deputy Assistant Chief Information Security Officer
Animal and Plant Health Inspection Service
United States Department of Agriculture