Privacy Impact Assessment

ISC Service Now Project

Policy, E-Government and Fair Information Practices

- Version: 1.1
- Date: March 20th, 2019

United States Department of Agriculture

Privacy Impact Assessment for the

ISC Service Now System

March 15, 2019

Contact Point

Brad Reighard
United States Department of Agriculture
816-518-4143

Reviewing Official

LaWanda Burnette
Privacy Analyst, ISC Privacy Team
United States Department of Agriculture
(314) 457-4728

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Information Security Center 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 Information Security Center (ISC) of the United States Department of Agriculture (USDA) is charged with protecting the USDA Networks and IT infrastructure from bad actors and information threats. 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 ISC. 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?

ISC ServiceNow collects name on behalf of the Government employee or Contractor in order to get IT service.

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

Sources of information come from USDA employees and contractors who use the ISC 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. The customer would be defined as any Employee or Contractor in USDA requesting services from ISC.

1.4 How is the information collected?

The information can be provided in 3 ways. Sent to helpdesk personnel or directly to the ticketing system as email; entered by the customer via the help desk portal page, or provided over the phone to helpdesk personnel.

1.5 How will the information be checked for accuracy?

When data is provided via email to personnel, it is checked for accuracy as it's transferred to the ticketing system
When data is provided via email to the system, it is not checked for accuracy, but later verified by helpdesk personnel.
When data is provided by the helpdesk portal page, the customer's name, business email address, and USDA agency are checked by the eAuth system.
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?

ISC does not purposefully collect PII.

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 using open fields in the ServiceNow portal was the primary privacy risk. Our Employees have been trained to not enter PII into the system, but we cannot guarantee customers will not add PII to the system. Privacy rights of the employees and external Privacy Impact Assessment ISC ServiceNow parties/persons will be protected by USDA, OCIO and ISC 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 ISC ServiceNow instance.
- All access to the system is controlled by the USDA eAuthentication 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.
- Any PII data other than Name added inadvertently by the customer or helpdesk employee will be redacted following the ISC PII ServiceNow Redaction procedure. The redaction process is started as soon as PII is discovered and should be completed within 3 business days.

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

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

N/A

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 ISC ServiceNow instance is protected through the use of eAuthentication 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?

Any PII data added inadvertently by the customer or helpdesk employee will be redacted following the ISC PII ServiceNow Redaction procedure.

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

Not Applicable

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

PII that is entered by un-trained users is removed upon discovery and not stored. The PII that is collected is specifically name only, and low risk 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?

Only Names are shared with other USDA organizations, therefore, the risk is minimal.

4.2 How is the information transmitted or disclosed?

Information is transmitted over https with authenticated users.

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.

Low, only authenticated users have access to Names.

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?

ISC helpdesk may contact the DHS and provide details of the incident in compliance with policy. Only the incident part of the ticket is shared.

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?

For certain incidents an email is sent to DHS alerting them of a new ticket. No attachments are sent.

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

ISC only collects Names, and no other PII. No attachments are sent.

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.

This system does not require a SORN.

6.2 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 customer's name is provided on a voluntary basis by the customer.

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

Yes, the system only requires their Name to create a new request or incident ticket.

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, 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.

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

No notice is provided.

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

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

The customer is contacted to correct the business email address. Business 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 ISC boundary

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

See 7.2

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

See 7.1

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 not 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?

Users must be authenticated through eAuth. At this point they will only have access to request tickets. They cannot access any other system functions. To access more system functions, they need to fill out a Service Access Request. This request must be approved by their Agency ISSPM, the ISC System Owner, and the ISC ISSPM. Once approved appropriate access roles are granted to the user.

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?

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?

There is an ATT. ISC is in the process of obtaining an ATO at the time of 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.
Encryption through HTTPS
System Audit Logs

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?

Low risk because ISC only collects Name information in the system.

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 ISC 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
- Service desk (incident management)
- Problem management
- Knowledge management
- Service request and service catalog
- 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, the ISSPM for ISC has reviewed these documents.

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

No 3rd party websites are used.

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

Responsible Officials

Brad Reighard, USDA OCIO ISC

United States Department of Agriculture

Approval Signature

Brad Rounding
Director, ASOD
OCIO/ISC/ASOD
United States Department of Agriculture