Privacy Impact Assessment
ServiceNow-ACFO

Technology, Planning, Architecture, & E-Government

- Version: 2.1
- Date: July 1, 2020

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

Service Now – ACFO System

July 1, 2020

Contact Point
Joe Giorlando
ACFO-SS-FMS-CSB
(504)-226-3539

Reviewing Official
Kenneth McDuffie
Information System Security Program Manager
USDA ACFO-SS-FMS
(504) 226-3417

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Assistance Chief Financial Officer – Financial Management Systems (ACFO-SS-FMS) ServiceNow system. The ServiceNow Software as a Service (SaaS) provides incident management capabilities. The PIA was conducted because the ServiceNow system has the potential to store personally identifiable information within the cloud provided solution.

Overview

System Name: ServiceNow

USDA Component: Office of the Chief Financial Officer

Purpose: ACFO-SS-FMS uses ServiceNow to track incidents. ServiceNow is a third party hosted cloud-based solution. ServiceNow is hosted outside of the ACFO-SS-FMS boundary. ACFO-SS-FMS currently uses ServiceNow as an incident tracking solution. If the incident cannot be solved a change request is generated outside of the Service Now solution. The actual change is accomplished outside of the Service Now application as well.

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?

ServiceNow-ACFO collects name, email address, and contact numbers, and PIV.

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

The sources of the information are USDA employees and contractors who use the ACFO-SS-FMS Financial Management Modernization Initiative (FMMI) system and wish to report incidents or requests for change.

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

The data is being collected in order to provide helpdesk service to FMMI users. The information may be used to create reports and other files related to customer query and incident response; query monitoring; and customer feedback records.

1.4 How is the information collected?

The information is either put into the ServiceNow system directly by the user or provided over the phone to helpdesk personnel.

1.5 How will the information be checked for accuracy?

When data is provided by the ServiceNow user directly into the system, it is not checked for accuracy. It is up to the user to ensure that the data that they are submitting is accurate.

When 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 from Active Directory when the correct customer is selected in the search box.

For eAuthentication (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?

Legal Authorities:
- 5 U.S.C. Section 301, Departmental regulations.
- 5 U.S.C. Chapter 57, Travel, Transportation, and Subsistence.
- 26 U.S.C. Section 6011, General requirement of return, statement, or list.
- 26 U.S.C Section 6109, Identifying Numbers.
    - 31 U.S.C. 3711 through 3719, Claims of the United States Government.

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, is the primary privacy risk. Privacy rights of employees and contractors will be protected by USDA and ACFO-SS-FMS by the following means:

- All access to the data in the system is controlled by formal authorization. Each user prior to be given a system account must be approved for the functional roles that are needed within the ACFO-SS-FMS ServiceNow instance.
- All access to the system is controlled by the eAuthentication application. No actions can be performed in the system without first authenticating.
- 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 prior to 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 collected is only used as contact information in order to provide incident management services to the customer. In the event that additional privacy information is uploaded into the ServiceNow system by a user it is to help clarify an incident that is occurring in the FMMI system and the information is not further utilized.

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

Not Applicable – 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 – system does not use commercial or publicly available data

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.

ServiceNow is protected via USDA eAuthentication which serves as a gateway for accessing the system. Information is protected through various levels of security and policy. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so within the application boundary.

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?

ServiceNow data is retained by ACFO-SS-FMS for one year after issue is resolved or when no longer needed for business use, whichever is appropriate. (See NARA General Records Schedule 5.8: Administrative Help Desk Records and https://www.ocio.usda.gov/policy-directives-records-forms/records-management/staff-office-file-plan)

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

Yes. Records are retained in accordance with NARA policies. (see above USDA DR 3080-001 and https://www.ocio.usda.gov/policy-directives-records-forms/records-management/staff-office-file-plan

Records Management, USDA DR-3090, Litigation Retention Policy for Documentary Materials including Electronically Stored Information, et al.

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

ACFO-SS-FMS has determined that the data retention periods and practices are adequate to safeguard PII.

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, ServiceNOW does not share with any other USDA system.

4.2 How is the information transmitted or disclosed?

Not Applicable, ServiceNOW does not share with any other USDA system.

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, ServiceNOW does not share with any other USDA system.

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, ServiceNOW does not share with any other USDA system.

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, ServiceNOW does not share with any other USDA system.

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

Not Applicable, ServiceNOW does not share with any other USDA system.

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

Not Applicable, ServiceNOW does not share with any other USDA system.

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 URS?

The system is covered under the OCFO-10 SORN.
https://www.federalregister.gov/documents/2018/12/31/2018-28375/privacy-act-of-1974-system-of-records

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

U.S. Government intention to collect PII data is declared in the System of Record Notices, OCFO-10 Financial Systems, made publicly available within the U.S. Federal register, as well as in the Privacy Act, and at data collection points throughout the Federal government. Individuals who enter their own PII data are notified of their rights and protections under the Privacy Act before providing information via those collection points, which are outside the scope of control of USDA ACFO-SS-FMS. If any PII data is provided into ServiceNow, it is provided on a voluntary basis directly by the individual into the system or via phone to the helpdesk.

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

Individuals are given the opportunity and the right to decline provision, based upon protections and limitations in various U.S. Regulations, Acts, guidelines, policies, etc., at the myriad points of collection. If any PII data is provided into ServiceNow, it is provided on a voluntary basis directly by the individual into the system or via phone to the helpdesk.

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

Individuals consent to particular uses of the information at the time of provision. Grievances involving consent and unauthorized use of the information can be addressed to the collecting Government agency, to agencies listed within applicable System of Record notices, or through other legal means.

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 ACFO-SS-FMS 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 obtain information regarding the procedures for gaining access to their own records contained within ServiceNow by submitting a request to the Privacy Act Officer, 1400 Independence Avenue, SW, South Building, Washington, DC 20250. The envelope, and all letters contained therein, should bear the words "Privacy Act Request." A request for information should contain the name of the individual, the individual's correspondence address, the name of the system of records, the year(s) of the records in question, and any other pertinent information to help identify the file(s). This is further explained in SORN OCFO-10, Financial Systems.

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

Procedures for contesting records are the same as procedures for record access in section 7.1 above. Include the reason for contesting the record and the proposed amendment to the information, including any supporting documentation that shows how the record is inaccurate.

For information such as email address or phone number, the customer is contacted to correct the email address. Phone numbers are verified when a customer calls into the help desk. The data is checked for accuracy by the customer when directly entering ticket information into the self-service portal. For eAuthentication related system access and transactions, eAuth does this externally and is not part of the ServiceNow-ACFO system boundary. Further information is in SORN OCFO-10, Financial Systems.

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

Notification is provided in the system of records notice available in the Federal Register. See OCFO-10, Financial Systems. Procedures for contesting records are the same as procedures for record access in section 7.1 above. Include the reason for contesting the record and the proposed amendment to the information, including any supporting documentation that shows how the record is inaccurate.

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

If formal redress is not possible after contacting USDA in accordance with established procedures, individuals are directed to utilize other legal measures to correct erroneous information, including but not limited, filing civil and/or criminal complaints. See OCFO-10, Financial Systems.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Individuals concerned that their PII data may have been compromised may contact the USDA office designated within the System of Records Notice posted in the U.S. Federal Register. See SORN OCFO-10, Financial Systems. Internal employees may also contact their respective Human Resources and/or Privacy Office representative for further assistance.

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?

The system contains automated workflows that can be customized to provide a minimum level of compliant access. This access is based on an individual's relationship with the USDA (.e. having an identity record in the USDA HR system or Level 2 elevation by Local Registration Authority). Other levels of access can be granted with supervisor approval or approval from a higher level authority. All access transactions, including approvals, additions, or removals of access are fully logged by the system.

8.2 Will Department contractors have access to the system?

Yes, there are USDA contractors that have access to ServiceNow.

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

All USDA employees and contractors receive annual security awareness training that includes specific training regarding the protection of PII. Privileged users are required to take additional, more detailed security training commensurate with their access permissions.

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

The system has been formerly Accredited through the Risk Management Framework process of the USDA. CSAM contains all the proper documentation. The Authority to Operate date is May 3, 2019 with an expiration date of May 3, 2022.

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 access the system; no temporary or guest accounts are permitted. Auditing is turned on for the system and audit logs are periodically reviewed for indications of misuse.

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 no significant risks associated with the information collected by ServiceNow. There is no data sharing of PII and all personnel accessing the ServiceNow system are cleared and trained annually on the proper handling and protection of PII 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?

ServiceNow is considered an ACFO-SS-FMS system.

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

ServiceNow does not use technology that would prompt an increase in concern regarding privacy protection. ServiceNow is a commercial off-the-shelf product that has gone through robust security verification by both government and commercial agencies.

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 ServiceNow system owner and ISSPM have reviewed both OMB M-10-22 and M-10-23.

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

The use of the ServiceNow enterprise cloud was a result of OMB Memorandum M-12-10 to shift to commodity IT.

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

No PII will become available through the user of the 3rd party website and application.

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

Agency Responsible Officials

JOSEPH GIORLANDO Digitally signed by JOSEPH GIORLANDO Date: 2020.08.20 09:56:17 -05'00'

Joe Giorlando Date
Acting Director, Customer Services Division
Office of the Chief Financial Officer
Financial Management Services
United States Department of Agriculture

KENNETH MCDUFFIE Digitally signed by KENNETH MCDUFFIE Date: 2020.08.17 09:30:09 -05'00'

Kenneth B. McDuffie Date
Information System Security Program Manger
Associate Chief Financial Officer/Shared Services
Financial Management Services
United States Department of Agriculture

Agency Approval Signature

LANCE RAYMOND Digitally signed by LANCE RAYMOND Date: 2020.08.21 13:33:00 -05'00'

Lance D. Raymond, PhD Date
Office of the Chief Financial Officer
Associate Chief Financial Officer for
Shared Services
Director, Financial Management Services
United States Department of Agriculture