Privacy Impact Assessment
NFC Business Service Management-ServiceNow

NFC Business Service Management-ServiceNow

- Version: 1.1
- Date: May 2018
- USDA National Finance Center

United States Department of Agriculture

Privacy Impact Assessment for the

NFC Business Service Management-ServiceNow

May 2018

Contact Point

Justyn Worrell
USDA OCFO NFC
504-426-2064

Reviewing Official

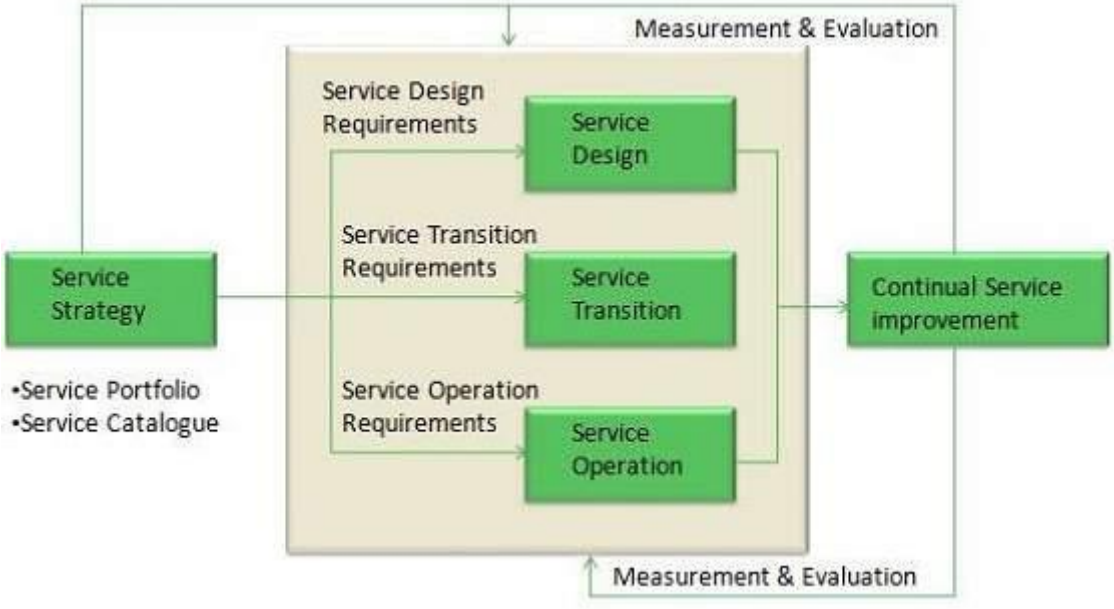
Ivan Jackson
NFC Privacy Officer
United States Department of Agriculture
(504) 426-7551

Abstract

The National Finance Center (NFC) Business Service Management-ServiceNow (BSM SNOW) solution is to replace the existing help desk solution and integrate and centralize multiple business processes and disciplines. Using a defined IT Infrastructure Library (ITIL)-compliant strategy, this solution will automate the management of Assets, Service Desk, Changes, Configuration, Releases, Knowledge, Financial, Performance, Service Levels, Capacity and Availability. This PIA is being conducted for the NFC BSM SNOW implementation of ITIL Service Strategy, Service Design, and Service Transition focusing on Transition Planning and Support, Service Asset and Configuration Management, Information Security Management, Capacity Management, and Financial Management for IT services.

Overview

NFC BSM SNOW system is a cloud service-provided Software as a Service (SaaS) application that is FedRAMP certified. It is owned by NFC Information Technology Services Division (ITSD). NFC BSM SNOW was selected to replace the BMC product lines currently in use at NFC. The key is that operational capabilities of all customer service offerings under the NFC Enterprise be realized. Access is equally important to internal and external customers who have a good understanding of the differences between a configuration and a customization in NFC BSM SNOW system. ITIL incorporates people, partners, processes and products using 5 key principles or disciplines – Service Strategy, Service Design, Service Transition, Service Operation and Continuous Process Improvement. A "Service" under ITIL is defined as, "A means of delivering value to customers by facilitating the outcomes that the customers want to achieve without the ownership of specific costs and risks."



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 includes various service requests for support, reported issues and supporting documentation. Supporting documentation varies per the type of request and may include names, phone numbers, addresses, date of birth, social security number, tax identification number, passport number, driver's license number, credit card numbers, bank account numbers, photographic image/identifying characteristics, handwriting or an image of the signature and employment history. The information is secured in an encrypted SQL database.

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

Sources of information are standardized OPM or Agency sanctioned and regulated forms used for various processes. Agents and consumers typically supply data to the system via the Employee Self Service web portal, phone, facsimile, U.S. Postal mail, and/or in person.

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

Information is collected for verification/validation purposes dealing with multiple service requests such as human resources requests and user account creation/maintenance.

1.4 How is the information collected?

Customers report an issue or submit a service request and attach form(s). If the attached documentation includes PII, customers are required to encrypt all documents with a unique password designated per each agency/customer.

1.5 How will the information be checked for accuracy?

Customer/users are responsible for the accuracy and completeness of any personal data provided.

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

5 U.S.C. Sec. 552a governs the collection, use and safeguarding of data collected on Individuals; 5 U.S.C. 301 (referenced in System of Record Notice [SORN] OP-1); Chief Financial Officers Act of 1990 (referenced in SORN OCFO-10); 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107 (referenced in SORN GOVT-1). The Form I-9, Employment Eligibility Verification, references the following: the Immigration Reform and Control Act of 1986, the Immigration Act of 1990, and the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

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

Most data collected are primarily included in standardized forms. If these forms require PII to be visible, then the document must always be encrypted. Risk is the failure of the agent not following NFC's agreed upon processes and procedures.

The NFC Contact Center (NCC) procedures require that any attachments to emails or Requester Console tickets that contain PII must be encrypted prior to being sent for processing. If the NCC receives an attachment that is not properly encrypted with a password, the attachment is immediately encrypted and the ticket is closed. The Agency that sent the request is notified of the PII incident and the need to send another request using authorized procedures. NFC's Incident Response Team is also notified in accordance with current guidelines.

Additionally, all Agency Security Officers (ASO) and Operations and Security Center (OSC) agents are authorized to attach PII data only if the attachment is encrypted and password protected. If the submitting official does not encrypt and password protect the document, the receiving agent sends a response that the service request will be closed and must resubmitted by the ASO with the correct encrypted and password protected documentation attached. In addition, the receiving agent submits a request to the system administrators to remove the PII from the system. The receiving system administrator sends a confirmation notice to the agent regarding the removal of the record. NFC's Incident Response team is also notified of the removal of the unencrypted PII document.

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.

Information is used to track and monitor various application systems and deliver various service request for all participating agencies who have an agreement with NFC. The data is used for multiple types of service offerings from payroll/personnel, financial, technical and security systems. For example, access request for Mainframe or Mid-Range systems.

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

Internal ServiceNow Analytics application. Dashboards, metric charting and forecast analysis are a few of the reporting features used from analysis data. However, PII within attachments will not be used in the analysis process; data is encrypted and stored in the system only and used as a reference for the agency. The metadata produced will not contain PII.

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.

When a customer includes an attached document, the NFC BSM SNOW application will automatically provide a notification to the customer that all documentation containing PII must be encrypted.

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?

Depends on each business unit but typical retention is seven years.

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

Yes. The retention period is in line with the agency's policy related to records retention, and complies with the standards set forth by NARA.

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

Very minimal risk is involved. NFC's SaaS providers have multiple controls in place to protect the data and recover 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?

All internal organizations share information based on the reported issue.

4.2 How is the information transmitted or disclosed?

Information is only available via the SaaS provided solution and to those with the correct credentials to review and/or transmit data.

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.

Each business unit has submitted roles and behavior disclosure statements and privacy protection statements. All violations which put the agency at risk are reported and documented. Depending on the severity of the violation, user's privileges are reduced and retraining and re-certification is required.

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?

The only information shared externally is NFC's performance metrics for each customer agency. No PII is shared externally.

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 Does this system require a SORN and if so, please provide SORN name and URL.

Yes. The information stored within NFC BSM SNOW is covered under three existing SORNS.

OP-1 covers NFC's Payroll/Personnel-related systems.
OCFO-10 covers the NFC Administrative Billings and Collections System.
GOVT-1 covers the NFC Direct Premium Remittance System and the OPM Federal Employees Health Benefits Centralized Enrollment Clearinghouse System.

OP-1:
https://www.ocio.usda.gov/sites/default/files/docs/2012/OP%20-%201.txt

OCFO-10:
https://www.ocio.usda.gov/sites/default/files/docs/2012/OCFO-10.txt

GOVT-1:
https://www.ocio.usda.gov/sites/default/files/docs/2012/GOVT-1_General_Personnel_Records.txt

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

The agencies that employ individuals are responsible for obtaining authorization to collect use, maintain and share PII. NFC provides the agencies with the SORNs that are associated with NFC BSM SNOW. The agencies that use NFC BSM SNOW are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORNs. The individual employees must coordinate directly with their employing agency regarding these rights.

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

The agencies that employ individuals are responsible for providing individuals with the opportunity and/or right to decline to provide information, and also the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII. NFC provides the agencies with the SORNs that are associated with NFC BSM SNOW. The agencies that use NFC BSM SNOW are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORNs. The individual employees must coordinate directly with their employing agency regarding these rights.

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

NFC provides the agencies with the SORNs that are associated with NFC BSM SNOW. The agencies that use NFC BSM SNOW are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORNs. The agencies are responsible for informing their employees of their rights to consent to particular uses of their information, as described in the SORNs. The individual employees must coordinate directly with their employing agency regarding these rights.

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.

NFC coordinates and communicates with the agencies that employ individuals, not directly with the employees. NFC provides the agencies with the SORNs that are associated with NFC BSM SNOW. The agencies that use NFC BSM SNOW are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORNs. The agencies are responsible for informing their employees of their rights to consent to particular uses of their information, as described in the SORNs. The individual employees must coordinate directly with their employing agency regarding these rights.

From a regulatory and management controls perspective, a copy of the redacted PIA is available on USDA's Office of the Chief Information Officer web site.

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?

Each individual will require a certain role assigned to the individual at the agency's discretion or per NFC security access guidelines.

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

If information is inaccurate or erroneous, an incident record is created to correct the information with supporting documentation.

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

At agency level, individuals are notified via email or during live conversation.

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

Notification primarily is via email; otherwise, a phone call is conducted.

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

Escalation procedures are in place where the authorized manager receives a request to redress or mitigate the reported issue. If warranted, NFC's incident response team is notified to execute their established action plan.

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?

Access requests are submitted by each agency's designated Agency Security Officer.

8.2 Will Department contractors have access to the system?

Yes, only if their Contracting Officer or Contracting Officer's Representative has submitted an access request after they have been adjudicated from personnel security.

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

Each end user will receive either paper-based or web-based training, which includes privacy, rules of behavior and security awareness.

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

In process.

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

Every record in this system will have an audit record from cradle to grave.

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?

A Risk Assessment was performed on NFC BSM SNOW and security controls have been documented in the System Security Plan. These controls are tested annually under the continuous monitoring and SSAE 18 programs.

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?

NFC BSM SNOW is an ITIL capital investment system utilizing a cloud service provider.

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

There are no known privacy concerns with the technology currently employed.

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?

NFC BSM SNOW does not use third party websites or applications.

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?

No.

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

Not applicable.

10.12 <u>Privacy Impact Analysis</u>: 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

MARIA JOLLEY

Digitally signed by MARIA JOLLEY
Date: 2018.05.22 11:00:26 -05'00'

System Manager/Owner
Maria Jolley
Associate Director of Operations
Information Technology Services Division
USDA National Finance Center

MICHAEL CAMPBELL

Digitally signed by MICHAEL CAMPBELL
Date: 2018.05.22 13:44:40 -05'00'

Project Manager
Michael Campbell
Financial Management Office
USDA National Finance Center

IVAN JACKSON

Digitally signed by IVAN JACKSON
Date: 2018.06.25 13:11:55 -05'00'

NFC Privacy Officer / ISSPM / CISO
Ivan R. Jackson
Associate Director of Information Technology Security
Information Technology Services Division
USDA National Finance Center

Agency Approval Signatures

IVAN JACKSON

Digitally signed by IVAN JACKSON
Date: 2018.07.25 16:05:17 -05'00'

Anita Fincher
Authorizing Official Designated Representative
Anita H. Fincher, Director
Information Technology Services Division
United States Department of Agriculture