USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	NFC Business Service Management - ServiceNow
Program Office	USDA-OCIO-DAITO
Mission Area	DAITO-OCFO-NFC
CSAM Number	2224
Date Submitted for Review	08/20/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Nija Enclarde	318-955-1393
Information System Security Manager	Tracy Haskins	202-720-8245
System/Program Managers	Anh Lewellen	504-258-1636

Abstract

The Privacy Impact Assessment (PIA) is for the United States Department of Agriculture (USDA), Office of Chief Financial Officer (OCFO) - National Finance Center

Business Service Management -ServiceNow® (NFC BSM SN) solution. The ServiceNow®Software as a Service (SaaS) provides service desk solutions which integrate and centralize multiple business processes and disciplines for internal and external customer agencies. The PIA was conducted because ServiceNow SaaS can store personally identifiable information in secured attachments within the cloud provided solution

Overview

NFC BSM SN system is a cloud service-provided SaaS application that is FedRAMP certified. The subscription service is owned by NFC's Government Employee Service Division (GESD). NFC BSM SN provides shared service offerings such as external payroll for agencies, and the Office of Personnel Management (OPM) partners associated with all NFC, and OCIO's customer service offerings that include HR, payroll, time and attendance solutions under the NFC Enterprise. 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 SN system. A "Service" under Information Technology Infrastructure Library (ITIL) terms 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: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

What legal authorities and/or agreements permit the collection of information by the project or system?

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.

Has Authorization and Accreditation (A&A) been completed for the system?

Yes

What System of Records Notice(s) (SORN(s)) apply to the information?

- OP-1: Privacy Act of 1974; Revision of 1974; Revision of System of Records
- OCFO-10: Privacy Act of 1974: System of Records
- GOVT-1: NFC Administrative Billings and Collections System

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.

Is the collection of information covered by the Paperwork Reduction Act?

Yes

Section 2: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

What information is collected, used, disseminated, or maintained in the system/program?

Identifying Numbers:

- Social Security number
- Driver's License number
- Passport number
- Taxpayer Identification number
- Credit/Debit Card number
- Personal Bank Account number
- Personal Mobile number

Biographical Information:

- Name (Including Nicknames)
- Date of Birth (MM/DD/YY)
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Employment Information

Biometrics:

- Fingerprints

Distinguishing Features:

- Palm Prints
- Photos

Characteristics:

- Scars, Marks, Tattoos

What are the sources of the information in the system/program?

Sources of information are standardized Office of Personnel Management (OPM) or Agency sanctioned and regulated forms used for various processes that include regulatory standard forms from OPM, USDA and NFC. Authorized Agency Agents and consumers typically supply data attachments to the system via secured web portals, applications, phone, facsimile, U.S. Postal mail, and/or in person.

How is the information collected?

Customers report a case, an issue or submit a service request and at times include an attached form(s). If the attached documentation includes PII, authorized customers are issued encryption token keys when submitting any document with PII data for all unique submission types.

Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

Not applicable

How will the information be checked for accuracy? How often will it be checked?

Customer/users are responsible for the accuracy and completeness of any personal data provided. Information is checked when updates are provided. However, for customer access to their created data records are assessed every 30, 60, and 120 days based on their inactivity. If access has been inactive for over 120 days, then access is revoked for ITIL licensed users.

Does the system/program use third-party websites?

Not applicable

What is the purpose of the use of third-party websites?

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

What PII will be made available to the agency though the use of third-party websites?

Not applicable

Privacy Impact Analysis: Related to characterization of the information.

Privacy Risk: Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Mitigation: Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Section 3: Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

Information is used to track and monitor various application systems and deliver various service requests 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 requests for Mainframe or Mid-Range systems.

Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

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.

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk: Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Mitigation: All attachments are encrypted upon submission for each type of service. If the submitting agent does not have an encryption key associated to their profile, a warning banner displays for any documentation being attached to be protected before submission. All NFC BSM SN instance environments are protected using eAUTH for USDA Federated access or User ID/Password for Non-Federated Authorized accounts with Government ReCAPTCHA for Multi-Factor Authentication (MFA).

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

How does the project/program/system provide notice to individuals prior to collection?

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 SN. The agencies that use NFC BSM SN 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 employment agency regarding these rights.

What options are available for individuals to consent, decline, or opt out of the project?

The agencies that employ individuals are responsible for providing individuals with the opportunity and/or right to decline to provide information, and 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 SN. The agencies that use NFC BSM SN 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 employment agency regarding these rights.

Privacy Impact Analysis: Related to notice.

Privacy Risk: Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Mitigation: NFC provides the agencies with the SORNs that are associated with NFC BSM SN. The agencies that use NFC BSM SN 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 use their information, as described in the SORNs. The individual employees must coordinate directly with their employment agency regarding these rights. NFC coordinates and communicates with the agencies that employ individuals, not directly with the employees.

Section 5: Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

What information is retained and for how long?

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

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Yes, inherited from Payroll/Personnel enterprise. The retention period is in line with the agency's policy related to records retention and complies with the standards set forth by NARA. General Records Schedule 2.2: Employee Management Records (GRS 2.2) scheduled depends on type of record.

Privacy Impact Analysis: Related to retention of information.

Privacy Risk: Excessive Data Retention: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

Data Breaches: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Mitigation: Data Retention Policy: Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes.

Regular Reviews: Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.

NFC's BSM SN authorized system administrators are issued an authorization (via a SN task) from Office of Chief Information Officer (OCIO) Information System Security Group (ISSG) Incident Response Team (IRT) to redact exposed PII data in all impacted tables. NFC's SaaS providers have multiple controls in place to protect the data and recover data.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

All internal organizations share information based on the reported issue.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: Each business unit has signed rules of behavior disclosure statements and privacy protection statements. All violations which put the agency at risk are reported and documented.

Mitigation: Depending on the severity of the violation, user's privileges are reduced and retraining, and re-certification is required.

With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

The only information shared externally is NFC's performance metrics for each customer agency and data provided to USDA's Data Analytics Team. It is important to note that no data provided does not include ANY personal information, simply counts and dates, no PII is shared externally.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: Not applicable

Mitigation: Not applicable

Section 7: Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

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 by NFC security access guidelines. Applicable SORN also lists procedures that allow individuals to gain access to their information.

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. Applicable SORN also lists procedures for correcting inaccurate or erroneous information.

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

At agency level, individuals are notified via email or during live conversation and the applicable SORN.

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

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

Privacy Impact Analysis: Related to redress.

Privacy Risk: Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Mitigation: Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

Escalation procedures are in place where the authorized manager receives a request to redress or mitigate the reported issue. If warranted, OCIO's Cyber Security, on behalf of NFC, executes their incident response team's established action plan.

Section 8: Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

How is the information in the system/project/program secured?

Every record in this system will have an audit record from cradle to grave. And all transactions are stored in multiple back-end systems and transaction log files at the host site. OCIO is running Microsoft Defender for Cloud Applications (MDCA) on all our NFC BSM SN cloud environments.

What procedures are in place to determine which users may access the program or system/project, and are they documented?

Access requests are submitted by each agency's designated Agency Security Officer or Security Coordinator. Request is documented via various forms that are attached to System Access Requests (SARs).

How does the program review and approve information sharing requirements?

All internal organizations share information based on the reported issue. The only information shared externally is NFC's performance metrics for each customer agency and data provided to USDA's Data Analytics Team. It is important to note that no data provided does not include ANY personal information, simply counts and dates, no PII is shared externally.

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

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