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	Web Applications (WebAPPS)
Program Office	National Finance Center
Mission Area	DAITO/OCFO-NFC
CSAM Number	1047
Date Submitted for Review	08/04/2025

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	Trudy Sandefer	504-426-1178

Abstract

NFC is a Shared Service Center (SSC) under the OPM Human Resources Line of Business (HRLOB). To carry out its wide-ranging responsibilities, the U. S. Department of Agriculture (USDA), and its employees and managers have access to diverse and complex automated information systems, which include system file servers, local and wide area networks running various platforms, and telecommunications systems to include communication equipment.

USDA relies on its information technology systems, including the Web Applications (WebApps), to accomplish its mission of providing cost-effective and reliable services to the USDA, other Federal agencies, and the public at large.

The National Finance Center (NFC) Government Employees Services Division (GESD), which falls under the United States Department of Agriculture (USDA), is responsible for development, deployment, maintenance, and testing of the NFC Web Applications (WebApps) major application (MA). This Privacy Impact Assessment (PIA) is being conducted to fulfill the requirements of Section 208 of Public Law 107-347 (the E-Government Act of 2002).

Overview

NFC Web Applications (Web Apps) include various subsystems that are menu driven, and whose mission is to provide online entry and query functions, perform edits to ensure that data entry meets established specifications and provides reports. The following subsystems are used for data entry, inquiry, correction, and reporting of data in Web Apps: Central Accounting Control System (CNTL) allows internal NFC users to access their records to add, update, or delete data. Working Capital Fund and Greenbook Online (FUND) users are allowed to access their records to add, update, or delete data. Reporting Center (RPCT) provides web-based reporting capabilities for agencies serviced by the NFC. OCFO Biennial Review of Charges for Things of Value (OFEE) provides agency personnel with the ability to review user fees, including loan processing fees, and to hold agency CFOs accountable for reporting the results of the reviews to the Department's OCFO. Intradepartmental Transactions Reconciliation System (ITRS) allows identification, reconciliation and reporting of intradepartmental transactions to facilitate elimination of intradepartmental balances for the consolidated financial statements. Pre-Authorized Debit System (PADS) allows authorized users to add, view, and update enrollee records that are sent to the United States Department of Treasury's Pay.gov system to process electronic preauthorized debit collections. General Ledger Interactive Description System (GLID) allows internal NFC users to access their records to add, update, or delete data. Tribal Insurance Processing System (TIPS) processes Federal Employees' Health Benefits (FEHB) and Federal Employees' Group Life Insurance (FEGLI) for employees of tribes, tribal organizations, and Urban Indian organizations. SecureAll (SALL) provides the capability for OCIO/ISC/ITSD Access Management Branch (AMB) and Agency Security Officers to establish, monitor and maintain security access to NFC's Web-based systems.

The following WebApps subsystems collect, process, generate, or store PII: PADS, SALL, TIPS, and RPCT.

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 (Public Law 101-576)- This act is cited as the primary authority for the USDA to collect, maintain, and use information through its financial systems, which includes NFC systems.

Title 5 of the U.S. Code, Chapters 53, 55, and 81- This section of the U.S. Code covers various aspects of government employees, including compensation, pay administration, and workers' compensation, all of which require the collection of PII.

Executive Order 9397- This executive order requires federal agencies to use a uniform identification system for individuals, which historically led to the use of Social Security Numbers (SSNs) for federal personnel. It is one of the legal justifications for collecting this sensitive PII.

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

Yes, it expires 5/14/2025.

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

Yes, OCFO/NFC-1, Systems for Personnel, Payroll, and Time & Attendance.

PADS, SALL, TIPS, and RPCT follow the OCFO/NFC-1, Systems for Personnel, Payroll, and Time & Attendance, SORN as reference. In addition, PADS and TIPS related to DPRS will follow the GOVT-1 SORN

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
- Passport number
- Employee Identification 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)
- Country of Birth
- City or County of Birth
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Children Information
- Mother's Maiden Name
- Personal Email Address
- Employment Information
- Alias (Username/Screenname)

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

Individuals and agencies can provide data for use in the system.

How is the information collected?

Information is collected via a web-based application directly from individuals, customers, and agencies. Agencies submit data via Connect: Direct and secure FTP over a VPN connection.

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

All information is provided by the individual, customer, or agency and does not use commercial or publicly available data.

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

Extensive error-checking routines are built into applications accessed via NFC- Web services. This includes record counts and database status checking.

Does the system/program use third-party websites?

No

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

Not applicable

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: Over-Collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: Implement access controls based on the classification of information, ensuring that only authorized personnel can access sensitive data.

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?

The information collected is used to assist individuals, customers and agencies with the processing of payroll information, personnel actions, FEHB benefits, and TIPS applications. The process includes hiring, separating, promoting, awards, work status, employee locator, performance evaluation, pay and leave calculation, insurance, health benefits, retirement, etc.

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.

WebApps has data validation routines built into the interface that checks for required fields, data types, and data ranges. Additionally, the business logic layer processes data before it is committed to the database, checking the data against business logic for accuracy and consistency. Individuals and agencies may run predefined and custom reports against the data and have the ability to access data elements depending on access privileges requested by authorized agency personnel.

Privacy Impact Analysis: Related to uses of the information.

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

Mitigation: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

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 NFC customers are responsible for providing notice to their employees prior to collection of PII. Individuals have the opportunity to decline to provide the information and are informed that the data is required to complete routine business functions.

All WebApps subsystems have a link to the privacy notice in the application landing page.

Privacy Act Notice

We are authorized to request this information under 5 U.S.C. Chapter 84. Executive Order 9397 authorizes us to ask for your Social Security number, which will be used to identify your account. We will use the information you provide to process the transaction you request on the NFC Web site.

You are not required by law to provide this information, but if you do not provide it, it may not be possible to process the actions you request on this Web site.

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

Individuals are provided with a consent statement, prior to logging into the application, via a warning banner which states:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, and seize any communication or data transiting or stored on this information system.

Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except USDA's Chief Information Officer.

Privacy Impact Analysis: Related to notice.

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

Mitigation: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

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?

The retention periods of data contained in this system are covered by NARA General Records Schedules. Civilian Personnel Records have various retention periods for specific types of data. These retention periods are adhered to per customer agency requirements and memorandum of understanding.

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.

This system complies with the guidance contained in the NARA General Records Schedules GRS 1.1, Financial Management and Reporting Records and GRS 3.2 Information Systems Security Records.

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 outlines how long different types of PII will be retained and the rationale for those timeframes.

The purpose of retaining the information is to provide historical data to respond to any issues including but not limited to payroll and benefit corrections, Equal Employment Opportunity (EEO) issues or lawsuits, and disciplinary actions. Retaining these records are in accordance with GRS I, which has a fairly limited retention period, to mitigate privacy risks associated with maintaining these records.

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?

Information collected by WebApps is owned by the individual and agency. The agency determines the use and sharing of the information. NFC does not share the data with any non-federal organizations; we maintain and secure the information on behalf of our customers.

WebApps is a Web-based application and uses 128-bit encryption HTTPS that is accessed by individuals, customers, and agency staff. WebApps uses Connect: Direct and secure file transfer (SFTP) over a VPN.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: Sharing PII without proper consent or outside the parameters set by privacy laws can result in legal penalties and reputational damage.

Mitigation: Limit the sharing of PII to only what is necessary for the intended purpose, adhering to the principle of data minimization.

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?

Pre-Authorized Debit System (PADS) shares Federal Employees Health Benefits (FEHB) insurance enrollees' personal information (such as name, address, place of employment, DOB) with the United States Department of Treasury (Pay.gov), so that Treasury may process electronic preauthorized debit collections for insurance.

TIPS (Tribal Insurance Processing System) is used to administer program enrollments, premium billings, and collections of Federal health and life insurance for TRIBES (Tribal Organizations and Urban Indian Organization's) employees. It shares PII as follows:

TIPS transmits insurance enrollees' information (such as name, address, DOB) to OPM, so that OPM can administer TRIBES enrollees' insurance with the FEHB carriers.

TIPS shares enrollees' information with the Department of Treasury RITS (Retirement and Insurance Transfer System) so that Treasury can process insurance billings and collections for TRIBES insurance.

On behalf of our customers, information is accessed via a Web-based application that uses 128-bit encryption HTTPS. Disclosure of information is restricted using role-based access, User IDs/passwords and sign on protocols.

Information is collected via a web-based application directly from individuals, customers, and agencies. Agencies submit data and file transfers via Connect: Direct and secure FTP over a VPN connection. Only individuals with an established "need-to-know" may access their specific profiled data.

Data is shared with the Department of Treasury using SSL (Secure Socket Layer 128 bit) communication lines.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Mitigation: Only authorized individuals can access information under the "need-to-know" policies. The proper controls are in place to protect the data and prevent unauthorized access.

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?

At the agency's discretion and according to the agency's security policies, individuals may be assigned a unique user id and password that allows them access to their own data in the system.

What are the procedures for correcting inaccurate or erroneous information?

Individuals with the proper assigned user role would be able to correct specific information themselves. However, most information in the system must be corrected by authorized users from the agency's payroll/personnel resources department at the request of the individual or by writing the agency.

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

Individuals with the proper assigned user role would be able to correct specific information themselves. However, most information in the system must be corrected by authorized users from the agency's payroll/personnel resources department at the request of the individual or by writing the agency.

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

Individuals with the proper assigned user role would be able to correct specific information themselves. However, most information in the system must be corrected by authorized users from the agency's payroll/personnel resources department at the request of the individual or by writing the agency.

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: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

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?

WebApps uses role-based access and User ID/password to protect access to data. Individuals only have access to their own records. Access to information is provided on a need-to-know basis and follows our "least privilege" policy. Top Secret, Secure All, and Oracle access is used to manage end user security. WebApps maintain strong role-based security controls.

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

The agencies determine user access. NFC follows Title VII, Chapter 11, Directive 2, Access Management, and Directive 58, Information Systems Security Program.

How does the program review and approve information sharing requirements?

Information Sharing between systems is pre-determined and goes through series of review and approvals via Interconnection Security Agreements (ISAs). Information sharing with users are strictly controlled and protected by user roles and responsibilities and needs to know basis.

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

Employees and contractors must complete annual security training and be properly trained in the system.