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	Payroll Accounting System (PAS)
Program Office	Office of Chief Financial Officer (OCFO)
Mission Area	DAITO / OCFO-NFC
CSAM Number	1045
Date Submitted for Review	09/16/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Nija Enclarde	318-599-1393
Information System Security Manager	Tracy Haskins	202-720-8245
System/Program Managers	Trudy Sandefer	504-426-7663

Abstract

The National Finance Center (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. The USDA relies on its information technology systems, including the Payroll Accounting System (PAS), to accomplish its mission of providing cost-effective and reliable services to the USDA, other Federal agencies, and the public at large. The 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 PAS 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

The function of the Payroll Accounting System (PAS) is to provide an internal financial management system of the U.S. Department of Agriculture (USDA), National Finance Center (NFC). PAS receives accounting transaction records generated by the NFC Payroll Personnel System (PPS). PPS processes biweekly payroll data for over 500,000 accounts including approximately 170 Federal agencies across all three Federal Branches (Executive, Legislative, Judicial), as well as several independent governmental agencies. PAS computes and reconciles payroll-appropriate charges; formats and feeds payroll related information to other systems; and produces numerous external and internal reports and Standard Forms (SF). PAS provides the data needed for reconciliation and accounting to other NFC major applications. PAS has two distinct, functional sides, accounting and reporting. Accounting and Budget Reports from several PAS subsystems (i.e., BCST, CAIS, DISB, SCAD, SCAP, and SCAR) are transmitted in files via FTP over a VPN between the NFC Mainframe and the Iron Mountain facility in Boyers, PA; and added to the Digital Records Center for Images (DRCI) system that Iron Mountain hosts.

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?

- Financial Systems is the Chief Financial Officers Act of 1990 (Pub. L. 101–576)
- eCFR Title 7, Agriculture, Subtitle B

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

Yes

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

The SORN is OCFO/NFC-1 Office of the Chief Financial Officer (OCFO), National Finance Center (NFC).

The agencies that employ individuals are responsible for obtaining authorization to collect, use, maintain and share PII. NFC provides the agencies with the System of Record Notice (SORN) that is associated with the NFC systems. The agencies that use NFC systems are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The individual employees must coordinate directly with their employment agency regarding these rights.

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

No

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
- Personal Bank Account number

Biographical Information:

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

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

Individuals and agencies can provide data for use in the system. PAS also receives data from other NFC Major Applications, as described in 6.1.

NFC shares PAS data with other USDA systems, as described below.

- NFC Administrative Billings and Collections (ABCO) – ABCO provides accounting data related to revenue, refunds, or reimbursements and provides weekly billings for administrative accounts receivable to the PAS (BCST, SCAP, and DISB).
- NFC Direct Premium Remittance System (DPRS) - DPRS provides accounting data (financial transactions) to PAS General Ledger (SCAP) and DISB.
- NFC Payroll/Personnel System (PPS) – PPS (PACS) sends all agency charged payroll transactions to PAS for processing and reporting to the agencies.
- NFC Miscellaneous Administrative Systems Group (ADMIN) – The Document Tracking System (DOTS) interfaces with Disbursing (DISB) system to reissue checks.
- NFC Web Applications (WepApps) MA (TIPS and Reporting Center) - TIPS provides accounting data (financial transactions) to PAS SCAP. Some SCAP financial data is loaded to the Oracle database used by the Reporting Center WebApps application.

How is the information collected?

The data in PAS is obtained from other NFC Major Applications. The Payroll Personnel System (PPS) provides detailed accounting data related to Payroll and Personnel processing, and ABCO provides accounting data related to revenue, refunds, or reimbursements.

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. PAS does not use commercial or publicly available data.

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

PAS application code provides reconciliation routines at the application level. These are maintained on the mainframe and applied to data entered and data transferred there. As personnel actions and payroll documents are processed each pay period, updated data replaces existing data elements on the PAS database. Extensive error-checking routines are built into applications including edits of data received, record counts and database status checking. The information in PAS obtained from PPS and ABCO was checked for accuracy by those applications when it was originally collected.

Does the system/program use third-party websites?

No

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

PAS does not use third party websites or applications

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

PAS does not use third party websites or applications

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?

The purpose of the data is to record, process, and report the personnel and payroll data for USDA and other Federal agencies. The purpose of the data in PAS is to enable it to function as the internal financial management and accounting system of the USDA NFC, as part of the Payroll and Personnel services that NFC provides to USDA and other Government agencies; and to provide data needed for reconciliation and accounting to other NFC major applications and some Department of Treasury 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.

Not applicable

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk: There is a potential risk of unauthorized access or misuse of sensitive information if role-based access controls, authentication measures (UserID/password), and "least privilege" policies are not properly implemented, monitored, or maintained.

Mitigation: Implement and regularly audit strict role-based access controls, enforce strong authentication requirements, and conduct periodic reviews of user permissions to ensure they align with the "least privilege" principle. Maintain and update security measures such as Top-Secret Security, DB2 Secure Table, and Windows file security to prevent unauthorized access.

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 System of Record Notice (SORN) that is associated with the NFC systems. The agencies that use NFC systems are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The individual employees must coordinate directly with their employment agency regarding these rights.

SORN: OCFO/NFC-1 Office of the Chief Financial Officer (OCFO), National Finance Center (NFC).

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 SORN that is associated with NFC systems. The agencies that use NFC systems are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The individual employees must coordinate directly with their employment agency regarding these rights.

Privacy Impact Analysis: Related to notice.

Privacy Risk: NFC coordinates and communicates with the agencies that employ individuals, not directly with the employees. NFC provides the agencies with the SORN that is associated with NFC systems. The agencies that use NFC applications are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The agencies are responsible for informing their employees of their rights to consent to particular uses of their information, as described in the SORN.

Mitigation: Transparency: Clearly outline what personal data is being collected, the purpose of data collection, how it will be used, and who it will be shared with.

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. NFC retains information in PAS in accordance with NFC Record Schedule N1- 106-10-7, which states a retention period of 56 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. NFC Record Schedule N1-106-10-7 has been approved

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.

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?

Authorized agency users of PAS have access to this data. This includes agencies whose payroll is processed by NFC. The customer agency security officers handle all requests for any information pertaining to user accounts/access based on supervisory requests. Access is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties/access their data. Accesses requested/determined by personnel/payroll offices who submit the data. NFC will grant authority to use/access PAS to individual users at the request of the agencies approved by the user's agency security officer.

NFC shares PAS data with other USDA systems, as described below.

- NFC Administrative Billings and Collections (ABCO) – ABCO provides accounting data related to revenue, refunds, or reimbursements and provides weekly billings for administrative accounts receivable to the PAS (BCST, SCAP, and DISB).
- NFC Direct Premium Remittance System (DPRS) - DPRS provides accounting data (financial transactions) to PAS General Ledger (SCAP) and DISB.
- NFC Payroll/Personnel System (PPS) – PPS (PACS) sends all agency charged payroll transactions to PAS for processing and reporting to the agencies.
- NFC Miscellaneous Administrative Systems Group (ADMIN) – The Document Tracking System (DOTS) interfaces with Disbursing (DISB) system to reissue checks.
- NFC Web Applications (WepApps) MA (TIPS and Reporting Center) - TIPS provides accounting data (financial transactions) to PAS SCAP. Some SCAP financial data is loaded to the Oracle database used by the Reporting Center WebApps application.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

Data Breaches: Internal systems can be vulnerable to breaches, compromising PII.

Mitigation: Data transmission risks are mitigated by the required use of secure file transmission methods for all information that is exchanged between PAS and another system, agency, or organization. The System Security Officer handles requests for information pertaining to user accounts. Access control is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties. Access is determined by the agency and based upon the application need and level to access the data.

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?

Information collected by PAS is owned by each agency. The agency determines the use and sharing of the information. NFC maintains and secures the information on behalf of our customers. Information is shared with the following external organizations:

- Department of Treasury Shared Accounting Module (SAM) - SAM updates PAS applications (SCAR and MASC) with valid Treasury Symbols via FTP over secure VPN from the Federal Reserve Bank (FRB) in St. Louis, so that PAS has the current valid Treasury Accounting Symbols needed to properly classify Federal financial transactions.
- Department of Treasury Payment Application Modernization (PAM) system – PAS/DISB sends data to PAM, via ConnectDirect. PAS provides individuals' name/address and payment amounts to PAM (and if electronic, the routing and account number and account type). The purpose is to inform Treasury how to issue the payment (electronically or paper check), to whom, and the amount of the payment.
- Iron Mountain Digital Records Center for images (DRCi) - Accounting and Budget Reports from several PAS subsystems (i.e., BCST, CAIS, DISB, SCAD, SCAP, and SCAR) are transmitted in files via FTP over a VPN between the NFC Mainframe and the Iron Mountain facility in Boyers, PA; and added to the DRCi system that Iron Mountain hosts. The purpose of storing reports/information at Iron Mountain is to provide historical data to respond to any future issues including but not limited to payroll and benefit accounting corrections, Equal Employment Opportunity (EEO) issues or lawsuits, and disciplinary actions

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: Unauthorized Access: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Data Breaches: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Mitigation: The System Security Officer handles requests for information pertaining to user accounts. Access control is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties. Access is determined by the agency and based upon the application need and level to access the data. Data transmission risks are mitigated by the required use of secure file transmission methods for all information that is exchanged between PAS and another system, agency, or organization.

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?

Information in the system must be corrected by authorized users from the agency's payroll/personnel human resources department at the request of the individual or at agency direction

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

Each agency using the system would provide this information to individuals.

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

Each agency using the system would provide this information to individuals.

Privacy Impact Analysis: Related to redress.

Privacy Risk: It is the responsibility of the agency to ensure that personnel with access to correct data on individuals have the proper clearances, position sensitivity designations, and appropriate system access to the data.

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

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?

These security controls are tested annually under continuous monitoring and documented in the System Security Plan (SSP), SSAE 18, and A-123 programs.

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. Only role-based access is granted. NFC follows Directive 58, Information Systems Security Program, and Directive 2, Access Management.

How does the program review and approve information sharing requirements?

Information is collected 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.

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

Privacy and PII training are included in the Security Awareness and Rules of Behavior training that is required for all federal employees and contractors annually. An exam is provided following the training, and the user must receive 70% or better to maintain or receive access to the information system. Some NFC staff members receive additional privacy training according to their role within NFC. Users must be properly trained on the system.