

Privacy Impact Assessment

Payroll/Personnel System

- Version: 1.7
- Date: 2/10/2022
- Prepared for: USDA, OCFO-
National Finance Center





Privacy Impact Assessment for the Payroll/Personnel System

February 10, 2022

Contact Point

**Trudy Sandefer
OCFO, National Finance Center
504-426-7663**

Reviewing Official

**Tracy Haskins
Information System Security Manager
United States Department of Agriculture
202-720-8245**

Abstract

The National Finance Center (NFC) is a Shared Service Center (SSC) under the OPM HumanResources 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, localand wide area networks running various platforms, and telecommunications systems to include communication equipment.

The USDA relies on its information technology systems, including the Payroll/Personnel System (PPS), to accomplish its mission of providing cost-effective and reliable services tothe USDA, other Federal agencies, and the public at large.

The NFC Government Employees Services Division (GESD), which falls under the UnitedStates Department of Agriculture (USDA), is responsible for development, deployment, maintenance, and testing of the NFC PPS major application (MA).

This Privacy Impact Assessment (PIA) is being conducted to fulfill the requirements ofSection 208 of Public Law 107-347 (the E-Government Act of 2002).

Overview

The Payroll/Personnel System (PPS) consists of personnel (Official Personnel Folders, Applicant Supply Files, performance files, retention lists, appeals, grievances, complaints,disciplinary, conflict of interest, health benefits, suggestion and incentive awards, accident,training, time and attendance, travel voucher data (USDA), and classification files) and payroll data needed to conform to all applicable laws, Government regulations and procedures, and the needs of the Department and agencies in carrying out their personnel management responsibilities.

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?

The system consists of personnel (Official Personnel Folders, Applicant Supply, Files, Name,Date of Birth, Address, SSN, Financial data, payroll/personnel history, time and

attendance, information included in teleworking agreements, and classification files) and payroll data needed to conform to all applicable laws, Government regulations and procedures, and the needs of the Department and agencies in carrying out their personnel management responsibilities.

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

Federal agencies, employees, contractors, managers, agency human resources offices, and agency payroll/personnel offices provide information for PPS.

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

The purpose of the data is to record, process, and report the personnel and payroll data for USDA and other Federal agencies.

1.4 How is the information collected?

Information is collected via data entry, front end interfaces, and web based applications from Federal agencies, employees, contractors, and affiliates. HR staff may enter information on an individual's behalf. Agencies may submit and receive data via Connect Direct and secure FTP over a VPN connection. Only individuals with an established "need-to-know" may access their specific profiled data.

1.5 How will the information be checked for accuracy?

Users are responsible for the accuracy and completeness of any personal data provided. The Employee Personal Page/Employee Self Service (EPP/ESS) application allows some users to access, review, and update or correct some of their PII, unless access is prohibited by law or regulation, or the burden or expense of providing access is disproportionate to any data protection risks at stake. All other information in PPS 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. Additionally, PPS 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 PPS database. Extensive error-checking routines are built into applications including edits of data received, record counts and database status checking.

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. Based upon our Service Level Agreements, NFC's Payroll/Personnel system

processes the necessary data provided by our customer agencies so that we can provide them the appropriate HR and payroll services.

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

NFC complies with the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA), to ensure that data is protected from unauthorized access, malicious or inadvertent modification, disclosure, and disruption.

NFC also works diligently to secure Personally Identifiable Information (PII) by requiring adequate training of employees and contractors that have access to the data. NFC provides the degree of protection (administrative, technical, and physical safeguards) for the data collected as prescribed by the Privacy Act of 1974, 5 U.S.C. Section 552a. NFC ensures all data included in data file transmissions are provided, received, and stored in a secure manner.

NFC protects, labels, and handles the data in accordance with 5 U.S.C. Section 552, Privacy act of 1974, as amended and applicable to agency regulations. All employees and contractors adhere to security requirements for handling and storing of Federal data as directed by the Electronic Government Act Title III, also known as FISMA. Employees have access only to their own records; managers have access only to employees they supervise; and agency HR staff have access only to their agency employee information (as determined by the agency).

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 purpose and routine uses of the data include recording, processing, and reporting the personnel and payroll data for USDA and other Federal agencies.

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

PPS 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.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

All information is provided by the individual, customer, or agency; PPS 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.

PPS uses role based access and UserID/password to protect access to data. Employees have access only to their own records; managers have access only to employees they supervise; and agency human resources staff have access only to their agency employee information (as determined by the agency). Access to information is provided on a need-to-know basis and follows our "least privilege" policy. Top Secret and Oracle access is used to manage end user security. PPS maintains strong role based security controls.

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?

The retention periods of data contained in this system are covered by NARA Records Control Schedule. 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 PPS in accordance with the Record Control Schedule N1-016-10-7, which states a retention period of 56 years.

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

Yes. Record Control Schedule N1-016-10-7 has been approved.

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

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 law suits, and disciplinary actions. To mitigate risks associated with unauthorized release of PPS data, NFC removes data from online systems when appropriate, and stores it offline at a federal records center or other authorized location, for the minimum amount of time required. NFC destroys data on paper and microfiche following the guidance and timelines in accordance with the Record Control Schedule N1-016-10-7.

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?

Information collected by the PPS is owned by each customer agency. The customer agency determines the use and sharing of the information. NFC maintains and secures the information on behalf of our customers. The system/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. Access is requested/determined by personnel/payroll offices who submit the data. NFC grants authority to use/access PPS to individual users at the request of the agencies approved by the user's ASO.

NFC shares our customers' PPS data with other NFC MAs (Major Applications), as described below.

1. NFC Administrative Billings and Collection System (ABCO): PPS (subsystems PAYE and ADJP) provides payroll and debt related data to ABCO.
2. NFC Payroll Accounting System (PAS): PPS (PACS) provides agency charged payroll transactions to PAS for reporting to the agencies.
3. NFC Web Applications (WebApps) - PPS sub-application WTWO generates data for transmission to the Reporting Center (a sub-application of the NFC WebApps MA).
4. EmpowHR: PPS (PINE) uses human resources data provided by EmpowHR.
5. Insight: PPS generate files for transmission to the Insight hosting environment for processing.
6. Miscellaneous Administrative Systems Group (ADMIN): The ADMIN Document Tracking System (DOTS) sub-application interfaces with the PPSPAYE sub-application to reissue checks.
7. OCIO eAuthentication (eAuth) application: The eAuthentication application provides authentication services for some PPS subcomponents (EPP/ESS and

EPPA). Authenticators are protected from unauthorized disclosure and modification by leveraging SSL/TLS encryption.

8. Financial Management Modernization Initiative (FMML): PPS (PACS) creates flat data files (including PII) for transmission to FMML.
9. Miscellaneous Income System (MINC): PPS (EARN) generates a file for transmission to the OCFO MINC application for use in producing 1099s.

4.2 How is the information transmitted or disclosed?

Information is collected via data entry and front end interfaces from individuals, customers and agencies. Agencies submit data via Connect Direct and files transfers that use secure FTP over a VPN connection. The web-based applications in PPS use 128-bit encryption HTTPS.

Information is shared with other USDA systems as described in 4.1 above.

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.

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. NFC grants authority to use/access PPS at the request of the customers and the requesting user's ASO. Employees have access only to their own records; managers have access only to employees they supervise; and agency human resources staff have access only to their agency employee information (as determined by the agency). Access is requested/determined by the agency payroll/personnel offices, 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 PPS and another system, agency, or organization.

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?

Information collected by the PPS is owned by each customer agency. The customer agency determines the use and sharing of the information. NFC maintains and secures the information on behalf of our customers.

- 1 Iron Mountain - Digital Records Center for images (DRCi) system: PPS sub-applications (SPPS, PACS, RETM, PAYE) generate files for transmission to the the Iron Mountain DRCi system. .
- 2 Equifax Workforce Solutions/TALX (The Work Number application): Payroll data generated from PPS/UCFE and an employment verification file generated by OCIO/DISC personnel from data stored in the PPS database are encrypted and then transferred via SecureFTP to a secure FTP server at Equifax. The Work Number application is a national employment verification service provided by Equifax to subscribers.
- 3 Treasury – Collections Information Repository (CIR)/Treasury Web Applications Infrastructure (TWAI): Files containing payroll and human resource data are produced by PPS (PAYE) for transmission to CIR/TWAI.
- 4 GDC Integration, Inc. (GDCI) - General Support System (GSS): PPS creates Employee Daily (PPS data) and TMGT 3 & TMGT 5 (Agency Contract Point data) files (including PII) for transmission to GDCI GSS for processing by the GDCI GSS Paycheck 8 application.

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.

Yes, the sharing of PII outside the Department is compatible with the original collection, and covered by a SORN. Please see Section 5.1 above. NFC follows the USDA/OP-1, Personnel and Payroll System for USDA Employees Customer agency SORN as reference. POAM ID: 22911.

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

Information is collected via data entry and front end interfaces from individuals, customers and agencies. Agencies submit and receive data via Connect: Direct and files transfers that use secure FTP over a VPN connection. The web-based applications in PPS use 128-bit encryption HTTPS. Any information transmitted from PPS to external systems must be transmitted via secure transmission, such as SFTP, over a Virtual Private Network (VPN) or other secure transmission protocols.

To Iron Mountain - Digital Records Center for images (DRCi) system: PPS electronic reports (files) are transmitted via FTP over a VPN between NFC Mainframe and the Iron Mountain facility in Boyers, PA.

To Equifax Workforce Solutions/TALX: Data is encrypted and then transferred viaSecureFTP to a secure FTP server at Equifax.

To Treasury – Collections Information Repository (CIR)/Treasury Web ApplicationsInfrastructure (TWAI): Files are transmitted from NFC Mainframe to Treasury in Kansas City, MO via Connect:Direct.

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

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. NFC grants authority to use/access PPS at the request of the customers and the requesting user's ASO. Employees have access only to their own records; managers have access only to employees they supervise; and agency human resources staff have access only to their agency employee information (as determined by the agency). Access is requested/determined by the agency payroll/personnel offices, and based upon the application need, and level to access the data. The proper controls are in place to protect the data and prevent unauthorized access.

Data transmission risks are mitigated by the required use of secure file transmission methods for all information that is transmitted from PPS to another system, agency, or organization.

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.

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 PPS. The agencies that use PPS 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 employing agency regarding these rights. POAM ID: 22911

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

The NFC customers are responsible for providing notice to their employees prior to collection of PII.

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 SORN that is associated with PPS. The agencies that use PPS 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 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 SORN that is associated with PPS. The agencies that use PPS 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. 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 SORN that is associated with PPS. The agencies that use PPS 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. 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?

At the customer 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 some PPS applications

7.2 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.

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

Each agency using the system would provide this information to its employees

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

Each agency using the system would provide this information to its employees

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

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. NFC access control procedures, role based security of the application, and agency reporting of individual access and utilization aid agency officials to mitigate the risks of agency individuals with improper access

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 agencies determine user access. Only role based access is granted. NFC follows Directive 58, Information Systems Security Program (Revision 3); and Directive 2, Access Management

8.2 Will Department contractors have access to the system?

Yes, if authorized a valid role

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

Privacy and PII training is 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.

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

Yes

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

PPS provides auditing at the application, database and network/operating system levels

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 PPS and security controls have been documented in the System Security Plan. These controls are tested annually under SSAE 18, and an independent assessment is performed every three years or when changes are made to the system

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?

The NFC Payroll/Personnel System is comprised of various subsystems that (1) are menu driven, (2) provide online entry and query functions, (3) perform edits to assure that data entry meets established specifications, and (4) provide reports. These applications interface with each other to form the integrated Payroll/Personnel System. This system, which

calculates payroll in two-week cycles, processes both electronically entered and system generated actions.

The NFC PPS MA resides primarily in an IBM Mainframe running the IBM z/OS operating system. PPS is implemented with COBOL batch programs developed by the NFC staff, and IDMS and DB2 databases located on logical partitions created and defined according to workload. The IDMS uses set theory to provide a special, tree-like hierarchy to support many-to-many relationships. This produces more tables in the database, simplifying table relationships. It also reduces modification anomalies, making the database more reliable.

The web-based applications in PPS consist of custom code and customized COTS applications running in a Windows environment. The applications were developed in ASP 3.0 and ASP.NET by the NFC staff; the webTA COTS application was developed by Kronos. The applications use relational database technology (DB2 and Oracle). The Windows-based servers provide interfaces to back-end databases on mainframe or midrange-based systems. The applications are connected to AIX, Solaris, or Red Hat Linux back-end database servers, and also to USDA NFC's enterprise mainframe

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

There are no privacy concerns with the technology employed. The PPS system is hosted in the NFC data center. PPS has undergone a detailed security vulnerability assessment and has been certified and authorized

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 utilizes Google Analytics as a Web measurement tool on the NFC Web Site, and in the PPS application called Employee Personnel Page (EPP). This tool is used to capture

the Internet domain and IP address from which users access our website, the type of browser and operating system used to access our site; the date and time a user accessed our site; the page the user visited; and whether the user linked to the NFC Web site from another website, the address of that website.

This information is used to help us make our site more useful, to learn about the number of visitors to our site, the types of technology our visitors are using to visit our Web site, and to present relevant information to users based on their Web site browsing requests.

We do not track user web activities beyond their browsing the NFC Web site. We do not cross reference browsing habits with other entities, and we do not sell or give away user information to other entities

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

No PII is captured

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)?

No

10.10 Does the system use web measurement and customization technology?

Yes, in the Employee Personnel Page (EPP) application only. NFC utilizes Google Analytics as our Web measurement tool. We currently are tracked under two main accounts – USDA's and NFC's. This tool is used to capture the Internet domain and IP address from which users access our website, the type of browser and operating system used to access our site; the date and time a user accessed our site; the pages the user visited; and whether the user linked to the NFC Web site from another website, the address of that website.

This information is used to help us make our site more useful, to learn about the number of visitors to our site, the types of technology our visitors are using to visit our Web site, and to present relevant information to users based on their Web site browsing requests.

We do not track user web activities beyond their browsing the NFC Web site. We do not cross reference browsing habits with other entities, and we do not sell or give away user information to other entities.

All of the above is outlined in our Privacy Policy located online at:

https://nfc.usda.gov/AdditionalResources/privacy_policy.php

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?

All of the information related to the collection of web site usage statistics and the use of Cookies is outlined in the NFC Privacy Policy available to all users at https://nfc.usda.gov/AdditionalResources/privacy_policy.php. The privacy policy also provides users with a link to the www.USA.gov for step by step instructions on web site measurement and customization opt-out.

NFC Privacy Policy at https://nfc.usda.gov/AdditionalResources/privacy_policy.php provides users with a link to the www.USA.gov for step by step instructions on web site measurement and customization opt-out

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

TRUDY SANDEFER  Digitally signed by
TRUDY SANDEFER
Date: 2022.02.10
12:50:34 -06'00'

Trudy Sandefer,
Information System Owner
OCFO, NFC
United States Department of Agriculture

Agency Approval Signature

TRACY
HASKINS  Digitally signed by
TRACY HASKINS
Date: 2022.04.06
17:42:05 -04'00'

Tracy Haskins
Information System Security Manager
OCIO, DAITO
United States Department of Agriculture