Privacy Impact Assessment

Payroll Accounting System (PAS)

- Version: 2.2
- Date: January 2018
- Prepared for: USDA National Finance Center (NFC)
- Payroll Accounting System (PAS)

United States Department of Agriculture

Privacy Impact Assessment for the

Payroll Accounting System (PAS)

January 2018

Contact Point
Trudy Sandefer, Acting Associate Director
Mainframe Applications Directorate
504-426-7663

Reviewing Official
Ivan Jackson, Associate Director
Information Technology Security Directorate
504-426-7551

USDA National Finance Center
United States Department of Agriculture

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 1.0 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, 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.

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

Individuals and agencies can provide data for use in the system. PAS also receives data from other NFC Major Applications, as described in 4.1.

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.

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.

1.4 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.

1.5 How will the information be checked for accuracy?

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.

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.

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 the Federal Information Security Management Act (FISMA).

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 processing and reporting the personnel and payroll accounting data for USDA and other Federal agencies, and providing data needed for reconciliation and accounting to other NFC major applications and some Department of Treasury systems.

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

PAS 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. PAS 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.

PAS uses role based access and UserID/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 Security, DB2 Secure Table and Windows file security are used to manage end user security. PAS 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 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.

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

Yes. NFC Record Schedule N1-106-10-7 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 for NFC to respond to any issues including but not limited to payroll and benefit accounting corrections, Equal Employment Opportunity (EEO) issues or law suits, and disciplinary actions. To mitigate risks associated with unauthorized release of 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 NFC Record Schedule N1-106-10-7.

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?

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. Access is 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.
- ACFO – PegaSys-USDA - On behalf of the United States Commission of Civil Rights (USCCR), the PAS Central Accounting Interface System (CAIS) transmits, via SFTP, summarized payroll accounting transactions (including Names and Social Security Numbers) to ACFO - Pegasys.

4.2 How is the information transmitted or disclosed?

Information is transmitted to other NFC 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. 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.

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 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 law suits, and disciplinary actions.

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.

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

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.

Information is transmitted to external systems as described in 5.1 above.

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

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

The agencies that employ individuals are responsible for obtaining authorization to collect, use, maintain and share PII. NFC provides the agencies with the 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 employing agency regarding these rights.

6.2 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 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 employing agency regarding these rights.

6.3 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 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 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.

6.4 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 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. 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 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.

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 individuals.

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

Please refer to Section 7.3.

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, 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. Users must be properly trained on the system.

8.4 Has Assessment & Authorization 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?

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

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

PAS is an accounting system.

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

No. PAS is an established mainframe application. PAS is implemented with COBOL batch programs, and DB2 and IDMS data base management systems. PAS inherits security protection implementations from the NFC Data Center and its supporting general support systems. Data security is achieved through resource allocation/access management implemented through Computer Associates' Top Secret (CA-TSS) software.

PAS 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?

PAS does not use third party websites or applications.

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

PAS does not use third party websites or applications.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

PAS does not use third party websites or applications.

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?

PAS does not use third party websites or applications.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

PAS does not use third party websites or applications.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

PAS does not use third party websites or applications.

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?

PAS does not use third party websites or applications.

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)?

PAS does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Not applicable.

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

Not applicable.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

Not applicable.

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.

PAS does not use third party websites or applications.

Agency Responsible Officials

TRUDY SANDEFER
Digitally signed by TRUDY SANDEFER
Date: 2018.03.23 13:28:53 -05'00'

System Manager/Owner
Trudy Sandefer, Associate Director
Mainframe Applications Directorate
Government Employees Services Division
USDA National Finance Center

Date

IVAN JACKSON
Digitally signed by IVAN JACKSON
Date: 2018.04.04 09:58:42 -05'00'

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

Date

Agency Approval Signature

DONNA SPEED
Digitally signed by DONNA SPEED
Date: 2018.05.08 10:18:57 -05'00'

Authorizing Official Designated Representative
Donna Speed, Deputy Director
Technical Services
Government Employees Services Division
USDA National Finance Center

Date