Privacy Impact Assessment

Web Applications (WebApps)

Version 9.5

September 2017

USDA, OCFO, National Finance Center

United States Department of Agriculture

Privacy Impact Assessment for the

WebApps (Services) Version 9. 5

September 2017

Contact Point
Debby Tatum, Associate Director
Web Applications Directorate
504-426-1102

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

USDA National Finance Center
United States Department of Agriculture

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.

The 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

WebApps is composed of 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 provide reports. The subsystems consist of payroll and personnel system, 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

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

Personal information such as, full name, address, phone number, place of birth, place of employment, dependent(s), social security number, bank routing numbers, bank accounting numbers is collected from employee at initiation of employment and throughout their Federal career as long as their employing agency is serviced by the National Finance Center (NFC). HR offices are also responsible for entering such data. Civilian applicant information is collected during enrollment in the Tribal Insurance Processing System (TIPS).

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

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

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

WebApps serves as a repository to store personnel and payroll data for the purpose of performing payroll/personnel operations, administration of records, health and billing on behalf of our customers.

1.4 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.

1.5 How will the information be checked for accuracy?

Extensive error-checking routines are built into applications accessed via NFC-Web services. This includes 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.

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

2.1 Describe all the uses of information.

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 processing include; hiring, separating, promoting, awards, work status, employee locator, performance evaluation, pay and leave calculation, insurance, health benefits, and retirement, etc.

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

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.

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 and 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.

WebApps 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, Secure All, and Oracle access is used to manage end user security. WebApps maintains strong role based security controls.

Section 3.0 Retention

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.

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

This system complies with the guidance contained in the NARA General Records Schedule 20, Electronic Records.

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. 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 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

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 organizations; we maintain and secure the information on behalf of our customers.

4.2 How is the information transmitted or disclosed?

WebApps is a Web-based application and uses l28-bit encryption HTTPS that is accessed by individuals, customers, and agency staff. WebApps uses Connect:Direct and secure file transfer (SFTP) over a VPN.

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.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

PADS shares 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.

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.

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?

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, UserIDs/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 shared with OPM and AWRC Post Master/Bacompt mail vendor is transmitted using FTP (File Transfer Protocol) over a secure VPN (Virtual Private Network). Data is shared with Health and Human Services CMS (Center for Medicare and Medicaid Services) and Department of Treasury using SSL (Secure Socket Layer 128 bit) communication lines.

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

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

Yes.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals have the opportunity to decline to provide the information and are informed that the data is required to complete routine business functions.

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.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

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

**********WARNING**********

1. 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.

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

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

1) 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.

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

3) 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.

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.

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. Individuals are notified several ways such as; by their agency, during online registration, during application use, etc. From the standpoint of an individual using the application, they are made aware of the collection of data and potential uses and must consent to both prior to accessing the system.

Section 7.0 Access, Redress and Correction

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?

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.

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

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

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

8.1 What procedures are in place to determine which users may access the system 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.

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.

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

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?

WebApps 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 WebApps and security controls have been documented in the System Security Plan. These security controls are tested annually under the continuous monitoring, SSAE 16, and A-123 programs.

Section 9.0 Technology

9.1 What type of project is the program or system?

WebApps consists of Payroll/Personnel, Billing, Health Benefits, and Insurance Programs and are in-house developed applications.

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

No; the WebApps major application 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 third-party websites and/or applications?

We use this information 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.

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

PII is not collected.

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

See 10.3

10.5 How will the PII that becomes available through the agency's use of third-party websites and/or applications be maintained and secured?

See 10.3

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

See 10.3

If so, is it done automatically?

See 10.3

If so, is it done on a recurring basis?

See 10.3

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

See 10.3

10.8 With whom will the PII that becomes available through the agency's use of third-party websites and/or applications be shared - either internally or externally?

See 10.3

10.9 Will the activities involving the PII that becomes available through the agency's use of third-party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

See 10.3

10.10 Does the system use web measurement and customization technology?

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://www.nfc.usda.gov/About_NFC/privacy_policy.html

GovDelivery is a comprehensive email subscription service that allows the public to "subscribe" to email notifications related to NFC and available from the NFC Website. It is a customizable service in the sense that a user can choose what information they wish to receive from NFC and customize how often they wish to receive it. This subscription service allows users to choose information that is specifically tailored to their needs and interests.

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

NFC GovDelivery account is renewed each year. During this renewal period the software and NFC's use of the software is assessed.

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.

Use of GovDelivery services requires the creation of a user profile; the user has the option to "Opt-out" of the subscription at any time. The only exceptions to this are the "private lists" used by NFC to ensure that communications are sent to certain personnel at agencies based on their role. Users listed in a private list cannot "opt-out" of receiving those specific communications from NFC.

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

Opting-out does not impact the user's acquisition of information and services.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of third-party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

See 10.3

Responsible Officials

DEBORAH TATUM

Digitally signed by DEBORAH TATUM
Date: 2017.09.19 09:11:51 -05'00'

System Manager/Owner
Debby Tatum, Associate Director
Web Applications Directorate
Government Employees Services Division (GESD)
USDA National Finance Center

TROY BRACKETT

Digitally signed by TROY BRACKETT
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=TROY BRACKETT, 0.9.2342.19200300.100.1.1=12001003425664
Date: 2017.09.20 13:35:14 -05'00'

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

Approval Signature

DONNA SPEED

Digitally signed by DONNA SPEED
Date: 2017.09.20 16:59:05 -05'00'

Authorizing Official Designated Representative
Donna L. Speed
Acting Director, Government Employees Services Division (GESD)
United States Department of Agriculture