Privacy Impact Assessment

for

HR SUPPORT Systems (HRSS)

Policy, E-Government and Fair Information Practices

Version: 1.1

Date: April 24, 2020

Prepared for: USDA FS CIO

Contact Point

Laree Edgecombe

System Owner

USDA NRE Forest Service

703-605-0820

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

The Forest Service Human Resources Support System (FS HRSS) is a General Support System (GSS) hosted at the National Information Technology Center (NITC) and supports the following HRM applications:

ConnectHR, Paycheck8, ePM, eForms, eTracker, LERIS, CRM and eMedical.

The E-Government Act requires agencies to conduct a PIA for systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public. This excludes agencies, instrumentalities or employees of the federal government. FS HRSS does NOT collect, maintain or disseminate information in identifiable form from or about members of the public. However, a PIA is being conducted as a best practice because the FS HRSS stores and maintains PII on employees.

Overview

The US Forest Service ASC-HRM-HRIS Staff maintains the FS HRSS General Support System. NITC is a framework of network components, servers, and infrastructure that provides the framework and platform for client applications. Components of GSS reside at GDCI's Primary Hosting Facility and GDCI's Alternate Hosting Facility

The purpose of the HRSS is to provide a single entry point for authentications into several disparate Human Resource (HR) programs that support the day to day activities of HR.

HRSS is a fully functional web-enabled system for HR applications used by FS employees to streamline and integrate existing business processes. The HR applications are described below:

ConnectHR is a multi-factor single-sign-on portal application specifically designed to meet the user management and authentication needs of Federal clients

Paycheck8: Time and Attendance recording and tracking system.

Paycheck Profile Manager (PPM): Allows Paycheck Administrators to review and manage employee details in the Paycheck Application.

ePM is a web-based system used for managing, processing, and tracking performance review completion and appraisals.

eForms is a web-based system used for on-boarding new hires and the associated forms management and provisioning requirements of the Agency or Department.

eTracker is a web-based system used for managing and processing personal action requests in accordance to the standards and guidelines set by the Office of Personnel Management (OPM).

LERIS is a web-based system used for case workflow management, case tracking, business process management, and reporting designed to meet the requirements of the global LER community and other specialized HR users.

eMedical is the Forest Service Qualifications system allowing Employee's and Administratively Determined employees the opportunity to track and record their progress through the Health Screening Questionnaire process and fire qualifications system.

CRM is a web-based system used for managing customer helpdesk tickets for both HRM and B&F.

All Applications Access:

USDA eGovernment-initiated eAuthentication system and GDCI's ConnectHR application provide user identification and authentication (IA) services for web-based users of client applications. There are two types of user access; GDCI System Administrators and Client End-Users. GDCI System Administrators have access to the GDCI platform operating system and are authenticated through GDCI Active Directory. Client End-Users only have access to the Client Applications and are authenticated through eAuthentication. There is no public access to any portion of the system.

The legal authority to operate the system comes from Executive orders 10450, 10577, 12968, 12968; 5 CFR Parts 5, 731, 732, 736; Title 5 USC Chapters 29, 33, 83, 84, 87, 89, 91.

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 Identification

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

Information collected includes personnel data such as name, financial data, and employment history name, and employment history, social security number, date of birth, tax withholding information, home address, and home number, and medical information.

1.2 Source

What is the source(s) of the information in the system?

The sources of information include the employees, their physicians, and the National Finance Center (NFC).

1.3 Justification

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

The information is collected, used, disseminated and maintained to allow for accurate processing of payroll, employment, and benefits information.

1.4 Collection

How is the information collected?

The information is collected from the employee through the completion of on-boarding forms such as W-4, I-9, and health and benefit forms.

1.5 Validation

How will the information be checked for accuracy?

HR Employees will validate against NFC System of Record (SORN) Personnel and Payroll System for USDA Employees USDA/OP-1.

1.6 Authority

What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The legal authority to operate the system comes from Executive orders 10450, 10577, 12968, 12968; 5 CFR Parts 5, 731, 732, 736; Title 5 USC Chapters 29, 33, 83, 84, 87, 89, 91.For additional Federal requirements for the collection of information, also see: 5 U.S.C. Chapter 552, 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management), and 18 U.S.C. 2071, 44 U.S.C. 3101 et seq., 44 U.S.C. 3506, Title 7 CFR 2.37, 36 CFR Chapter 12, Subchapter B, 36 CFR Part 1234, E-Government Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch. 36), OMB Circular A-130, NARA Disposition of Federal Records: A Records Management Handbook, NARA General Records Schedules.

1.7 Risk Mitigation

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Potential risk is loss of PII data including SSN and DOB that could lead to identity theft if the data was compromised. HRSS, as a GSS, employs the Microsoft Hardening guide for Server 2008 (Citation NIST SP - 800-43) and other National Institute of Standards and Technology (NIST) guidelines and therefore these risks are mitigated by the inherited security controls from HRSS.

This system of records collects the minimum amount of personally identifiable information necessary to verify the identity of those requesting information. Data is maintained in the information technology application, which is configured and maintained in accordance with policies and procedures established by the Forest Service.

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 Usage

Describe all the uses of information.

Personnel data required to complete business functions necessary to support the recruitment and management of personnel. Its uses include repetitive activities such as processing payroll transactions; determining retirement eligibility; dispensing monetary awards; detecting improper payments; garnishing wages, recording training plans, and so forth.

The typical Routine Uses are agreements for sharing personal information with:

To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation

To a congressional office

To the National Archives and Records Administration or other Federal government agencies

To an agency, organization, or individual for the purpose of performing audit or oversight operations

To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract

To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency

To the news media and the public

To appropriate agencies, entities, and persons when: FS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) or harm to the individual that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in

connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

2.2 Analysis and Production

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

None

2.3 Commercial/Public Use

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

None

2.4 Risk Mitigation

Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Security controls inherited from and access through e-Authentication will ensure information is accessed and handle only by those who have responsibility for the data. All reports generated by the system will only contain statistical data and therefore no PII.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 Time Period

How long is information retained?

The two file designation codes for this database will be 6130 - Employment Actions and 6100 - Personnel Operations/Statistical Reports. Retention for these two file codes will be as follows:

6130 - 5 years from the date of conversion, termination or separation 6100 - reports will be retained for 2 years from the date that the report is provided and printed.

3.2 Approval

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

Yes

3.3 Risk Mitigation

Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risks associated with the retention time is in accordance with the FS Records Management Policy

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). (http://www.ocio.usda.gov/records/policy.html DR 3080-1 Records Disposition)

FS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or agency that requested the personal records. These accounts are to be kept for five years, or the lifetime of the record, whichever is longer. Unless the records were shared for routine use purposes, the accounts of the disclosures should be available to the data subject upon request.

The disposition instructions in mission area, agency or staff office record schedules are mandatory. Officials may not dispose of records prior to their authorized disposal date or retain them beyond that date except in situations in which records might be relevant to pending or threatened litigation. If a program official determines that records need to be retained longer than authorized by the schedule, the mission area, agency or staff office records officer shall be contacted to obtain approval from NARA and, if necessary, to revise the schedule.

The actions taken regarding records and non-records no longer needed for current Government business include transfer to agency storage facilities or Federal records centers, transfer from one Federal agency to another, transfer of permanent records to the National Archives, and disposal of temporary records. For non-records, these actions include screening and destruction. Destruction is the primary type of disposal action and can include burning, shredding, deleting, or discarding with other waste materials. In the electronic realm, destruction is typically accomplished by overwriting or degaussing, depending on security requirements.

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 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

All personnel payroll and benefits information is shared with the National Finance Center.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Information is transmitted via a secure and encrypted (site to site) VPN tunnel.

4.3 Risk Mitigation

Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

A typical privacy risk is if the files were to be intercepted during transmission. This is mitigated through the files being transmitted over a secure and encrypted (site to site) VPN tunnel.

Risk: Customers should not send FS their personally identifying information. Customers are advised that they do not have to furnish the information but failure to do so may prevent their request from being processed. The information that customers furnish is almost never used for any purpose other than to process and respond to their request. However, FS may disclose information to a Congressional office in response to an inquiry made on behalf of the requestor, to the Department of Justice, a court, other tribunal when the information is relevant and necessary to litigation, or to a contractor or another Federal agency to help accomplish a function related to this process.

Mitigation: If shared within FS and the Department of Agriculture, all information is still used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of Agriculture have undergone a thorough background investigation. Access to facilities is typically controlled by

security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel.

Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

When a transaction must contain a signature in writing in order to be legally enforceable, due care is taken to ensure that documentation provides a record that is not subject to imperfect memory or competing claims as to what parties to the transactions intended.

The methods used to obtain, send, disclose and store information complies with applicable laws, such as those governing privacy, confidentiality, recordkeeping, and accessibility to persons with disabilities.

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 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

Information is shared with Department of Labor (DOL) for payment and processing of OWCP claims.

5.2 Compatibility

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, all use of PII share externally with DOL is covered under SOR USDA/OP-1 Personnel and Payroll System for USDA Employees.

5.3 Delivery and Security Measures

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

Information is shared via DOL's Electronic Data Delivery Interface (EDDI) which is a secure site to site encrypted VPN tunnel.

5.4 Risk Mitigation

Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

A typical privacy risk is if the files were to be intercepted during transmission. This is mitigated through the files being transmitted over a secure and encrypted (site to site) VPN tunnel.

Risk: Customers should not send FS their personally identifying information. Customers are advised that they do not have to furnish the information but failure to do so may prevent their request from being processed. The information that customers furnish is almost never used for any purpose other than to process and respond to their request. However, FS may disclose information to a Congressional office in response to an inquiry made on behalf of the requestor, to the Department of Justice, a court, other tribunal when the information is relevant and necessary to litigation, or to a contractor or another Federal agency to help accomplish a function related to this process.

Mitigation: If shared within FS and the Department of Agriculture, all information is still used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of Agriculture have undergone a thorough background investigation. Access to facilities is typically controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel.

Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

When a transaction must contain a signature in writing in order to be legally enforceable, due care is taken to ensure that documentation provides a record that is not subject to imperfect memory or competing claims as to what parties to the transactions intended.

The methods used to obtain, send, disclose and store information complies with applicable laws, such as those governing privacy, confidentiality, recordkeeping, and accessibility to persons with disabilities.

Section 6.0 System of Records Notice (SORN)

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 Requirement and Identification

Does this system require a SORN and if so, please provide SORN name and URL?

(Note: If a SORN is not required, answer "No" to this question, and "N/A" for questions 6.2 through 6.5.)

SORN USDA/OP-1 Personnel and Payroll System for USDA Employees.

SORN USDA/FS-15 Human Resources

6.2 Individual Notification

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

Employees of Federal government consent to the collection and use of their information when they agree to work for the government. Notice is also given when the employee enters information into the payroll and benefits system.

6.3 Right to Decline

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

No. The information is required to successfully obtain and maintain employment with the Federal Government.

6.4 Right of Consent

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

Employees of Federal government consent to the collection and use of their information when they agree to work for the government. Notice is also given when the employee enters information into the payroll and benefits system.

6.5 Risk Mitigation

Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Employees of Federal government consent to the collection and use of their information when they agree to work for the government. Notice is also given when the employee enters information into the payroll and benefits system. The notice offered at several times during employment is reasonable and adequate in relation to the system's purpose and uses, the confidentiality impact level of the PII, and capabilities for notice permissible within the system design. Data is verified upon entry into the system.

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 Access

What are the procedures that allow individuals to gain access to their information?

Employees can access some of the information via the Employee Personal Page at NFC.

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Data is verified upon entry into the system. System Administrators have the ability to update information once provided with corrected documentation. The system at NFC will also update incorrect information on a bi-weekly basis once a corrective action has been submitted and processed by NFC.

7.3 Notification

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

The employee would open a ticket with HR and the issue would be researched, documented and ultimately corrected.

7.4 Redress Alternatives

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

Not Applicable

7.5 Risk Mitigation

Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Upon an issue being raised, appropriate documentation would be required to ensure the new information is verified.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Procedures

What procedures are in place to determine which users may access the system and are they documented?

Access will be limited to HRM; eAuthentication assigns rolls and access. Controls are documented as part of the FS HRSS SSP.

8.2 Contractor Access

Will Department contractors have access to the system?

Yes. FS HRSS is housed at GDCII which is a Fee for Service contract.

8.3 Privacy Training

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

Privacy training is provided through required annual USDA Privacy and Computer Security Training for all end users. Additional Role Based Security Training is required for all employees both Forest Service and GDCII that have privileged use access.

8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer “Yes” and provide ATO expiration date(s).

This is a new system. Assessment & Authorization (A&A) is currently in process as of the writing of this PIA. This section will be updated with the Approval Authority to Operate (ATO) information once it is received.

8.5 Audit and Technical Safeguards

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

All data manipulation actions within HRSS are logged at the transaction level and abnormal activity is auto flagged and forwarded to all administrative personnel.

8.6 Risk Mitigation

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?

All PII leaving the facility is encrypted via AES256 or SSLV3. Physical access to the system requires electronic keycard, biometric access, and mechanical key.

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 Description

What type of project is the program or system?

Payroll and Benefits System

9.2 Privacy Concerns

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

Web access outside the Forest Service network. This is implemented with SSLV3 encryption and eAuthentication required for access.

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 Review

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 Purpose

What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

None

10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

None

10.4 PII Usage

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

N/A

10.5 PII Maintenance and Security

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 PII Purging

Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

N/A

10.7 PII Access

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

N/A

10.8 PII Sharing

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?

N/A

10.9 SORN Requirement

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)?

N/A

10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

10.11 Web Measurement and Customization Opt-In/Opt-Out

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

N/A

10.12 Risk Mitigation

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.

N/A

Responsible Official

LAREE EDGECOMBE Digitally signed by LAREE EDGECOMBE
Date: 2020.04.24 15:43:49 -04'00'

Laree Edgecombe
System Owner (SO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS Digitally signed by CYNTHIA TOWERS
Date: 2020.04.24 14:53:40 -05'00'

Cynthia Towers
Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

LAURA HILL Digitally signed by LAURA HILL
Date: 2020.04.28 12:05:11 -06'00'

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture