USDA Privacy Impact Assessment

Fiscal Year 2026

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Document created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	FS HR Support System (FS HRSS)
Program Office	Forest Service
Mission Area	Natural Resources and Environment (NRE) Forest Service (FS)
CSAM Number	2470
Date Submitted for Review	11/21/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Benjamin J Moreau	202-380-6165
Information System Security Manager	Kristopher Harig	208-954-2910
System/Program Managers	Teresa Rodriguez	505-563-9446

Abstract

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

Overview

The FS HR Support System (FS HRSS) is a fully functional web-enabled system for Human Resource (HR) applications used by FS employees to streamline and integrate existing business processes. These applications are provided as a Software as a Service (SaaS) solution by GDCI, Inc. The purpose of the FS HRSS is to provide a single-entry point for authentication into several disparate Human Resource programs that support the day-to-day activities of HR. The HR applications are described below:

- Connect Human Resources (ConnectHR) is a multi-factor single-sign-on portal application specifically designed to meet the user management and authentication needs of Forest Service employees.
- Paycheck8: Time and Attendance recording and tracking system.
- Electronic Performance Management (ePM) is a web-based system used for managing, processing, and tracking performance review completion and appraisals.
- Electronic Tracker (eTracker) is a web-based system used for managing and processing personal action requests in accordance with the standards and guidelines set by the Office of Personnel Management (OPM).
- Labor and Employee Relations Information System (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 Labor and Employee Relations (LER) community and other specialized HR users.
- Electronic Personal Security (ePS) is the system of record that houses and accounts for all records related to new hires (applicants) required pre-employment activities. These activities include: 1) Initiation/processing of required background investigations; 2) completion of pre-employment drug testing; and 3) applicants suitability determinations for determination of employment suitability.
- Electronic Medical (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.
- Workforce Restructuring and Placement System (WRAPS) is a system that can initiate a reorganization request, identify abolished positions and affect employees, and matches the affected employees to new available positions based on current or past work history and qualified preference positions while generating and documenting communications between Human Resources and employees.

Section 1: Authorities and Other Requirements

These questions identify all statutory and regulatory authorities for operating the project, application, or system, including the authority for collection, which SORN applies, if an ATO has been completed, and if there is Paperwork Reduction Act coverage:

What legal authorities and/or agreements permit the collection of information by the project, application, or system?

The legal authority to operate the system comes from Chief Financial Officer's Act of 1990.

Has Authorization and Accreditation (A&A) been completed for the project, application, or system?

Yes. Authority to Operate (ATO) granted on 8/24/2024.

Which System of Records Notices (SORNs) apply to the information?

OCFO/NFC-1 Systems for Personnel, Payroll, and Time & Attendance

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

No

Section 2: Information Characterization

These questions define the scope of the information requested and collected, as well as the reasons for its collection as part of the project, application, or system being developed:

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

Identifying Numbers

- Social Security Number
- Truncated or Partial Social Security Number
- File or Case ID Number
- Employee Identification Number
- Taxpayer Identification Number
- Personal Bank Account Number
- Personal Mobile Phone Number
- Health Plan Beneficiary Number

Biographical Information

- Name (Including Nicknames) Date of Birth
- Ethnicity
- Country of Birth
- City or County of Birth
- Citizenship
- Immigration Status
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Marital Status
- Spouse Information
- Child Information
- Military Service Information
- Race
- Nationality
- Mother's Maiden Name
- Personal Email Address
- Employment Information
- Alias (Username or Screenname)
- Personal Financial Information (Including Loan Information)
- Education Information
- Resume or Curriculum Vitae

Distinguishing Features

- Signatures

Medical and Emergency Information

- Medical or Health Information
- Mental Health Information
- Disability Information
- Workers' Compensation Information
- Patient ID Number
- Emergency Contact Information

Specific Information and File Types

- Personnel Files
- Law Enforcement Information
- Credit History Information
- Health Information
- Academic or Professional Background Information
- Civil or Criminal History Information/Police Record
- Case Files
- Security Clearance or Background Check
- Taxpayer or Tax Return Information

What are the sources of the information in the project, application, or system?

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

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.

Does the project, application, or system use information from commercial sources or publicly available data? If so, explain why it is used.

No

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

Data is verified upon entry into the system. System Administrators can update information once it has been provided with the 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.

Does the project, application, or system use third-party websites?

No

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

Not Applicable

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

Not Applicable

List the privacy risks and mitigations related to the characterization of the information.

Privacy Risk: Potential risk is loss of PII data including SSN and DOB that could lead to identity theft if the data were compromised.

Mitigation: GDCI employs the Microsoft Hardening guide and other National Institute of Standards and Technology (NIST) guidelines for their servers and therefore these risks are mitigated by the inherited security controls from GDCI. This system collects the minimum amount of personally identifiable information (PII) 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. In addition, all users of the system are required to take Information Security Awareness Training annually as well as acknowledge they have read and agree to the Rules of Behavior for using Government information systems. Both cover the use and handling of PII.

Section 3: Information Uses

These questions delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the project, application, or system's business purpose.

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:

- Another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a federal agency, when the Government is a party to the judicial or administrative proceeding.
- Officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting work conditions.
- The Merit Systems Protection Board or the Office of the Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of OPM rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions, as promulgated in 5 U.S.C. 1205 and 1206, and as specified in 5 U.S.C. 7503(c) and 5 U.S.C. 7513(e), or as may be authorized by law.
- The Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation
- A congressional office
- The National Archives and Records Administration or other Federal government agencies
- An agency, organization, or individual for the purpose of performing audit or oversight operations
- Contractors and their agents, grantees, experts, consultants, and others performing or working on a contract
- An appropriate Federal, State, tribal, local, international, or foreign law enforcement agency
- The news media and the public

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.

Does the project, application, or system use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No, the system does not use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly.

List the privacy risks and mitigations related to uses of the information.

Privacy Risk: Unauthorized access and use of data.

Mitigation: Security controls inherited from, and accessed through, e-Authentication will ensure information is accessed and handled 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 4: Notice

These questions are intended to provide notice to the individual of the scope of information collected, the right to consent to use of the information, and the right to decline to provide information.

How does the project, application, or system provide notice to individuals prior to collection?

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.

What options are available for individuals to consent, decline, or opt out of the project?

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. Individuals do not have the option to opt out or decline. The information is required to successfully obtain and maintain employment with the Federal Government.

List the privacy risks and mitigations related to notice.

Privacy Risk: Individuals unaware of the collection of their data.

Mitigation: 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 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 5: Data Retention

These questions outline how long information will be retained after the initial collection.

What information is retained and for how long?

ConnectHR- 6100 Employee Management Administrative Records- Temporary 3 years- DAA-GRS-2017-0007-0001

Paycheck8- 6160- Time and Attendance Records- Temporary 3 years- DAA-GRS-2016-0015-0003

ePM- 6140- Employee Performance Fill System (EPFS)- Temporary 4 years- DAA-GRS-2017-0007-0008

eTracker- 6100 Employee Management Administrative Records- Temporary 3 years- DAA-GRS-2017-0007-0001

LERIS-6230- Records Management Program- Temporary 6 years- DAA-GRS-2013-0002-0007

ePS -6230- Records Management Program- Temporary 6 years- DAA-GRS-2013-0002-0007

eMedical- 6130-Medical-EMF Temporary, or Short-Term Records Temporary 1 year- DAA-GRS-2017-0010-0010

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, indicate the name of the records retention schedule.

Chris Meadows has approved the retention period as recorded. Per Chris Meadows, the retention for this will be 6230 – Records Management – Intermediary Records (GRS 5.2/100 (DAA-GRS-2017-0003-0002).

List the privacy risks and mitigations related to data retention.

Privacy Risk: Premature disposition of records

Mitigation: 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). (Departmental Directives home page 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 6: Information Sharing

These questions define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared, received, and/or transmitted? What information is shared, received, and/or transmitted, and for what purpose? How is the information transmitted?

All personnel payroll and benefits information are shared with the National Finance Center. Information is transmitted via a secure and encrypted (site-to-site) VPN tunnel.

List the privacy risks and mitigations related to internal information sharing and disclosure.

Privacy Risk: A typical privacy risk is if the files were to be intercepted during transmission. Customers are advised that they do not have to furnish personally identifying 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: This is mitigated through the files being transmitted over a secure and encrypted (site-to-site) VPN tunnel. All information is used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized people. 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 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 comply with applicable laws, such as those governing privacy, confidentiality, recordkeeping, and accessibility to people with disabilities.

With which external organizations (outside USDA) is information shared, received, and/or transmitted? What information is shared, received and/or transmitted, and for what purpose? How is the information transmitted?

Information is shared with Department of Labor (DOL) for payment and processing of Office of Worker Compensation Program (OWCP) claims. Information is shared via DOL's Electronic Data Delivery Interface (EDDI) which is a secure site-to-site encrypted VPN tunnel.

List the privacy risks and mitigations related to external information sharing and disclosure.

Privacy Risk: A typical privacy risk is if the files were to be intercepted during transmission. Customers are advised that they do not have to furnish personally identifying 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: This is mitigated through the files being transmitted over a secure and encrypted (site-to-site) VPN tunnel. All information is used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized people. 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 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 comply with applicable laws, such as those governing privacy, confidentiality, recordkeeping, and accessibility to persons with disabilities.

Section 7: Redress

These questions address the individual's ability to ensure the accuracy of the information collected about him or her.

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

The Privacy Act grants individuals a right to access their records and any information pertaining to them that is contained in the agency systems of records. While the Privacy Act increases an individual's right to access the individual's own record, it restricts an individual's ability to access a record pertaining to someone else. The Privacy Act prohibits disclosure of records in a system of records to any person or agency, unless disclosure is pursuant to the prior written request by, or with the prior written consent of, the individual to whom the record pertains.

To make an Electronic Privacy Act Request, please visit the following link: USDA Public Access Link. This link will allow you to electronically complete your request.

The USDA Public Access Link (PAL) is a web portal that allows requestors to create, submit, and track the status of their FOIA and Privacy Act request(s). To use the system, the requestor must register and create a username and password. This system also provides remote identity proofing and authentication through login.gov for Privacy Act requests.

A requester seeking access to USDA records should provide sufficient information about himself or herself to enable components to resolve, in a timely manner, any issues that might arise as to the subject and scope of the request, and to deliver the response and, if appropriate, any records released in response to the request. Generally, this includes the name of the requester, name of the institution on whose behalf the request is being made, a phone number at which the requester might be contacted, an email address and/or postal mailing address, and a statement indicating willingness to pay any applicable processing fees.

A requester seeking access to USDA records must also provide a reasonable description of the records requested, as discussed in paragraph (c)(1) of this section.

What are the procedures for correcting inaccurate or erroneous information?

As mentioned in 7.1, Please visit the following link: USDA Public Access Link for correcting inaccurate or erroneous information.

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

Individuals are notified of the procedures for correcting their information through the listed SORN in section 1.3.

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

Formal redress is provided.

List the privacy risks and mitigations related to redress.

Privacy Risk: Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

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

Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

How is the information in the project, application, or system secured?

Information that is transmitted is secured via an encrypted (site-to-site) VPN tunnel. Information residing within the applications is protected by GDCI.

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

FS HRM submits an SF-52 Request for Personnel Action form to the National Finance Center (NFC). Data from the form is entered into the EmpowHR data repository by NFC. NFC generates an updated "Bear" file every 2 weeks with all updated personnel information. GDCII pulls the "Bear" file from a secure NFC FTP site over secure VPN. The information from the "Bear" file is used by GDCII to update user information and accesses to FS HRSS applications. The HR Action Code for each record in the "Bear" file determines whether access is created, enabled, modified, disabled, or removed. Controls are documented as part of the FS HRSS SSP.

How does the project, application, or system review and approve information sharing requirements?

Information sharing requirements are documented, reviewed, and approved as part of the Interconnection Security Agreements (ISAs) between HRSS and each system that GDCI shares information with.

Describe what privacy training is provided to users either generally or specifically relevant to the project, application, 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 GDCI, that have privileged use access. HR personnel also undergo bi-annual mandatory PII training.