USDA Privacy Impact Assessment

Fiscal Year 2024

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

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented 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	NRE FS Customer Relationship Manager New Hire Experience (NRE FS CRM NHE)
Program Office	Natural Resources and Environment (NRE)
Mission Area	Forest Service (FS)
CSAM Number	2639
Date Submitted for Review	April 2, 2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Benjamin Moreau	benjamin.moreau@usda.gov	202-720-3463
Information System Security Manager	Kristopher Harig	kristopher.harig@usda.gov	208-387-5170
System/Program Managers	Gregory Gibson	gregory.gibson@usda.gov	228-910-2325

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

The Natural Resources and Environment Forest Service Customer Relationship Manager New Hire Experience (NRE FS CRM NHE) consists of Customer Relationship Manager (CRM) and New Hire Experience (NHE) applications. Ownbackup (Own) is utilized as the backup solution.

CRM is the Forest Service solution to bring content center functions under one roof for Human Resource Management, Budget and Finance (including travel) and Harassment. CRM is a Case Management tool with communities & collaboration, knowledge management, process management, integration, and reporting & analytics capabilities for the three content centers.

Additional functionality of CRM is a customer self-service portal for ticket submissions and knowledge management resources such as frequently asked questions, quick reference guides, etc.

NHE is a centralized workflow tracking tool to provide status updates on a potential Forest Service new hire. NHE will provide status updates to the hiring manager and the new hire.

CRM and NHE utilize PII gathered from the public, federal employee and contactors in order to properly track cases and provide accurate case management.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

CRM and NHE are developed in the Salesforce Government Cloud Plus Federal Risk and Authorization Management Program (FedRAMP) which is located in Amazon Web Services (AWS) GovCloud East region. Ownbackup is developed in Own FedRAMP which is also located in AWS GovCloud East.

NRE FS CRM NHE is a platform utilized by the Forest Service Human Resource Management as a ticketing case management tool that tracks internal and external inquires for FS contact centers which include Human Resources, Budget and Finance, Travel, and Harassment. In general, the information gathered will be based on the customer's inquiry with the FS and may include Personally Identifiable Information (PII). Inquires can range from various program areas within the FS such as payroll, payments, benefits, reporting an incident/accident, hiring, applications, preemployment, workers compensation claims, student loan program, filing a harassment case, travel. Due to the wide variety of inquiries that can be made, NRE FS CRM NHE collects and uses a wide variety of PII to provide the public, federal employees and federal contractors with proper assistance in their inquiries.

CRM functions as a Case Management tool with communities & collaboration, knowledge management, process management, integration, and reporting & analytics capabilities. CRM has data integration from Paycheck8, eSafety, National Finance Center (NFC) Mainframe (includes BEAR and 102), and NFC EmpowHR. MuleSoft is used as the integrator to move data from the integrated systems to CRM. No data is stored in MuleSoft.

NHE provides hiring managers and new hires with the ability to receive updates and track progress within the hiring process. NHE has data integration from National Finance Center (NFC) Mainframe (includes Bi-Weekly Examination Analysis and Reporting System - BEAR and 102), NFC EmpowHR, eTracker, USA Staffing, USAccess, ePS, SharePoint, Aglearn, and eSafety. MuleSoft is used as the integrator to move data from the integrated systems to CRM. No data is stored in MuleSoft.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

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

In order to receive entitlements, benefits or payment from the government, an SSN or TIN is required by law.

OPM GOVT-1,General Personnel Records (77 FR 73694.* 80 FR 74815)
Authority for Maintenance of the System: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107

OPM/GOVT-2 Employee Performance File System Records (71 FR 35342.* 80 FR 74815) Authority for Maintenance of the System: 5 U.S.C. 4314(c)(1), Sections 1104, 3321, 4305, and 5405 of title 5, U.S. Code, and Executive Order 12107

OPM GOVT-5 Recruiting, Examining and Placement Records (79 FR 16834.* 80 FR 74815) Authority for Maintenance of the System: Executive Order 12564 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

OPM/GOVT-10 Employee Medical File Systems Records (75 FR 35099.* 80 FR 74815) Authority for Maintenance of the System: Executive Orders 12107, 12196, and 12564 and 5 U.S.C. chapters 11, 33, and 63.

OCFO/NFC-1 Systems for Personnel, Payroll, and Time & Attendance (89 FR 5481) Authority for Maintenance of the System: The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Pub. L. 104–193); Chief Financial Officers Act of 1990 Pub. L. 101-576.

DOL/GOVT-1 Office of Workers' Compensation Programs, Federal Employees' Compensation Act File (81 FR 2576)6 Authority for Maintenance of the System:5 U.S.C. 8101 et seq., 20 CFR 1.1 et seq., FECA, Sections 8131-8132 of FECA, Federal Tort Claims Act

1.2. Has Authorization and Accreditation (A&A) been completed for the system?

Yes

Please provide the following:

1. The Security Plan Status: Approved

2. The Security Plan Status Date: 06/07/2024

3. The Authorization Termination Date: 06/07/2027

4. The Risk Review Completion Date: 06/07/2024

5. The FIPS 199 classification of the system (MODERATE)

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

OPM GOVT-1, OPM GOVT-2, OPM GOVT-5, OPM GOVT-10; DOL GOVT-1; OCFO/NFC-1

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

No

Section 2: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers

☒ Social Security number	☒ Truncated or Partial Social Security number	☒ Driver's License number
☒ Passport number	☒ License Plate number	☒ Registration number
☒ File/Case ID number	☒ Student ID number	☒ Federal Student Aid number
☒ Employee Identification number	☒ Alien Registration number	☒ DOD ID number
☒ Professional License number	☒ Taxpayer Identification number	☒ Business Taxpayer Identification number (sole proprietor)
☒ Credit/Debit Card number	☒ Business Credit Card number (sole proprietor)	☒ Vehicle Identification number
☒ Business Vehicle Identification number (sole proprietor)	☒ Personal Bank Account number	☒ Business Bank Account number (sole proprietor)
☒ Personal Device Identifiers or Serial numbers	☒ Business Device Identifiers or Serial numbers (sole proprietor)	☒ Personal Mobile number

☒ Health Plan Beneficiary number

☒ Business Mobile number (sole proprietor)

☒ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)

☒ Business Mailing Address (sole proprietor)

☒ Date of Birth (MM/DD/YY)

☒ Ethnicity

☒ Business Phone or Fax Number (sole proprietor)

☒ Country of Birth

☒ City or County of Birth

☒ Group Organization/Membership

☐ Religion/Religious Preference

☒ Citizenship

☒ Immigration Status

☒ Home Phone or Fax Number

☒ Home Address

☒ ZIP Code

☒ Marital Status

☒ Spouse Information

☒ Children Information

☒ Military Service Information

☒ Race

☒ Nationality

☒ Mother's Maiden Name

☒ Personal Email Address

☐ Business Email Address

☒ Global Positioning System (GPS)/Location Data

☒ Employment Information

☒ Alias (Username/Screenname)

☒ Personal Financial Information (Including loan information)

☒ Education Information

☒ Resume or Curriculum Vitae

☒ Business Financial Information (Including loan information)

☐ Professional/Personal References

Biometrics

☒ Fingerprints

☒ Hair Color

☐ DNA Sample or Profile

☒ Retina/Iris Scans

☒ Video Recording

Distinguishing Features

☒ Palm Prints
☒ Eye Color
☒ Signatures
☒ Dental Profile
☒ Photos

Characteristics

☒ Vascular Scans
☒ Height
☒ Weight
☒ Scars, Marks, Tattoos
☒ Voice/Audio Recording

Device Information

☒ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)
☒ Cell Tower Records (e.g., Logs, User Location, Time)
☒ Network Communication Data

Medical /Emergency Information

☒ Medical/Health Information
☒ Mental Health Information
☒ Disability Information
☒ Workers' Compensation Information
☒ Patient ID Number
☒ Emergency Contact Information

Specific Information/File Types

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

Sex (Male or Female)

2.2. What are the sources of the information in the system/program?

CRM Information is integrated with the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, Paycheck8, FS eSafety. If information is not readily available, the individual may be required to provide only if it is necessary to complete inquiries with the FS.

NHE Information is integrated with the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, FS eTracker, OPM USA Jobs, OPM USA Staffing, USAccess, FS ePS, USDA AgLearn, FS eSafety, USDA log.gov, and USDA ICAM Shared Services formally known as eAuthentication. If information is not readily available, the individual may be required to provide only if it is necessary to complete inquiries with the FS.

If information is not readily available through data integration, the individual may be required to provide additional information if it is necessary to complete inquiries with the FS. The individual could be a member of the public, FS employee, or contractor.

2.2.1. How is the information collected?

CRM Information is integrated with MuleSoft for internal information transmission from the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, Paycheck8, FS eSafety. If information is not readily available, the individual may be required to provide it only if it is necessary to complete inquiries with the FS.

NHE Information is integrated with MuleSoft for internal information transmission from the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, FS eTracker, OPM USA Jobs, OPM USA Staffing, USAccess, FS ePS, USDA AgLearn, FS eSafety, USDA log.gov, and USDA ICAM Shared Services formally known as eAuthentication. If information is not readily available, the individual may be required to provide it only if it is necessary to complete inquiries with the FS.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

Not Applicable.

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

Information is validated constantly through automatic data integration conducted by NFC, whichis the system of recording and will auto populate information automatically.

2.5. Does the system/program use third-party websites?

No

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

Not Applicable

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

Not Applicable

2.6. **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: By implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

Section 3: Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

The information in CRM is used for: case management capabilities across content centers for Human Resource Management, Harassment, Travel, Budget and Finance to track cases through completion and to maintain records.

The information in NHE is used for providing hiring managers and new hires with the ability to receive updates and track progress within the hiring process.

3.2. Does the system/project/program 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.

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Mitigation: By implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

The U.S Government's intention to collect PII data is declared in the System of Record Notices listed in 1.1, which are made publicly available within the Federal Register. Notice is also given at data collection points throughout the federal government. Employees of the 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.

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

Employees of the 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. There is no option for Federal employes to opt out, as the information is required to successfully obtain and maintain employment with the Federal Government.

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: There is an associated risk with the notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information that the users will not understand the notice or where to find it.

Mitigation: The notice to the individual provides the scope of information collected, the right to consent to use the information, and the right to decline to provide information prior to login. USDA also gives notice through the applicable SORNs.

Section 5: Data Retention

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

5.1. What information is retained and for how long?

6100 Personnel Operations/Statistical Reports - Temporary 2 years- DAA-GRS-2017-0007-0001 The information retained under Personnel Operations/Statistical Reports is HRM helpdesk tickets reports.

6130- Employment Actions Temporary 5 year- DAA-GRS-2017-0010-0010. The information retained under Employment temporary actions is information related to HRM Helpdesk ticketing and contains PII.

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

6100 Personnel Operations/Statistical Reports - Temporary 2 years- DAA-GRS-2017-0007-0001 The information retained under Personnel Operations/Statistical Reports is HRM helpdesk tickets reports.

6130- Employment Actions Temporary 5 year- DAA-GRS-2017-0010-0010. The information retained under Employment temporary actions is information related to HRM Helpdesk ticketing and contains PII.

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: The risk associated with retention of information being retained longer than necessary. CRM NHE aligns with National Archive and Records Administration (NARA) requirements.

Mitigation: FS has determined that the data retention periods and practices are adequate to safeguard PII while ensuring that mission critical data is available to support system restoration in the event of unplanned outages. CRM NHE aligns with NARA requirements.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

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

CRM Information is integrated with MuleSoft for information transmission from the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, Paycheck8, FS eSafety

NHE Information is integrated with MuleSoft for information transmission from the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, FS eTracker, OPM USA Jobs, OPM USA Staffing, USAccess, FS ePS, USDA AgLearn, FS eSafety, USDA log.gov, and USDA ICAM Shared Services.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Privacy risks associated with internal sharing and disclosure include:

Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

Data Breaches: Internal systems can be vulnerable to breaches, compromising PII.

Insider Threats: Employees with malicious intent may exploit their access to PII for personal gain.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Access Controls: Implement role-based access controls to limit who can access PII based on their job responsibilities.

Encryption: Use encryption for data in transit and at rest to protect PII from unauthorized access.

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

Not Applicable.

6.4. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: Not Applicable.

Mitigation: Not Applicable.

Section 7: Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

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

Data integration allows for individual information to be prepopulated from the USDA National Finance Center. Individuals can also view their data by accessing the National Finance Center Employee Personal Page or by Office of Personnel Management (OPM) electronic Official Personnel Folder (eOPF). Human Resource systems utilize limited personal information to conduct and complete your HR transactional needs. If your populated information needs to be updated or corrected contact your Forest Service Human Resource Department at 1-877-372- 7248 option 2. For additional information on USDA Privacy Policy please visit https://www.dm.usda.gov/privacy/index.htm.

7.2. What are the procedures for correcting inaccurate or erroneous information?

In the event that the information in OPM eOPF or USDA National Finance Center prepopulated information is inaccurate, and individuals are advised to contract the Forest Service Human Resource Department. A correction will be made at the system of record which will then repopulate the correct information. Human Resource systems utilize limited personal information to conduct and complete your HR transactional needs. If your populated information needs to be updated or corrected contact your Forest Service Human Resource Department at 1-877-372-7248 option 2. For additional information on USDA Privacy Policy please visit https://www.dm.usda.gov/privacy/index.htm.

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

Individuals are advised prior to log in to contact the Forest Service Human Resource Department in the event that a correction is needed. The banner states "Human Resource systems utilize limited personal information to conduct and complete your HR transactional needs. If your populated information needs to be updated or corrected contact your Forest Service Human Resource Department at 1-877-372-7248 option 2. For additional information on USDA Privacy Policy please visit https://www.dm.usda.gov/privacy/index.htm

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

Not Applicable.

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

Privacy Risk: Privacy Act risks associated with redress include:

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.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Failure to Address Complaints: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

Delayed Responses: Slow responses to redress requests can frustrate individuals and exacerbate feelings of mistrust and dissatisfaction, potentially leading to reputational harm.

Mitigation: By implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

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

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

Dedicated Privacy Officer/Privacy Point of Contact: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

Section 8: Auditing and Accountability

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

8.1. How is the information in the system/project/program secured?

PII is encrypted in CRM/NHE, access controls are in place to ensure only need-to-know individuals have access, and all users must authenticate through e-auth or login.gov to access CRM/NHE.

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

Each user in CRM/NHE has a limited and specific set of roles. Each role is defined such that it only gives access to the data needed for that role. Therefore, the definition of the role prevents a user from misusing the data.

8.3. How does the program review and approve information sharing requirements?

There are no significant risks associated with the internal sharing of PII data. All personnel accessing CRM/NHE PII data are cleared and trained annually on the proper handling and protection of PII data. The system itself is protected by role-based access layers and positive identification techniques such as multi-factor authentication to ensure only people authorized to view and act upon information about others can do so.

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

All CRM/internal NHE users receive annual security awareness training that includes specific training regarding the protection of PII. Privileged users within NRE FS are required to take additional, more detailed security training commensurate with their access permissions.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 5/19/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

Signed:____

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed:____

Gregory Gibson
System Owner (SO)
Natural Resources and Environmental, Forest Service System Owner
U.S. Department of Agriculture

Signed:____

Benjamin Moreau
Privacy Officer (PO)
Natural Resources and Environmental, Forest Service
U.S. Department of Agriculture

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.06.25 23:30:04 -04'00'

Signed:____

Office of the CPO Chief Privacy Officer (CPO)
U.S. Department of Agriculture