# 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 | 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 Forest Service eSafety (NRE FS eSafety) |
| Program Office | - |
| Mission Area | Natural Resources and Environment Forest Service |
| CSAM Number | 2549 |
| Date Submitted for Review | 12/12/2025 |

# Mission Area System/Program Contacts

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

# Abstract

eSafety is the Forest Service (FS) case management tool used to manage, track, and report incidents for the Office of Workers' Compensation Programs (OWCP) and Office of Safety and Occupational Health (OSOH). There are two separate Authority to Operate for eSafety. This narrative is for the front-end Natural Resources and Environment (NRE) FS eSafety. NRE FS eSafety is responsible for end user access controls as well as all data elements within eSafety. Origami Risk eSafety (OReS) is the backend which is responsible for the operation of the system.

NRE FS eSafety uses United States Department of Agriculture (USDA) mandatory Multi-Factor Authentication (MFA), USDA Identity, Credential and Access Management (ICAM) Shared Services, formally known as eAuthentication for method of login. When an end user logs in using USDA ICAM Shared Services, their information will prepopulate using USDA Human Resource data integration. Non data integrated end user will use a Uniform Resource Locator (URL) using any internet web-browser to manually enter all data fields in eSafety. End users of eSafety can be employees, Administratively Determined (AD) employees, contractors, affiliates, interns, volunteers, and fellows. NRE FS eSafety is not used by the public.

NRE FS eSafety consists of the end user data maintained in Origami Risk eSafety as well as limiting the access and safeguarding the data. NRE FS eSafety is responsible for session, presentation and application layer management as outlined within the NRE FS eSafety SSP and Control Implementation tab of the CSAM entry.

# Overview

The Forest Service (FS) of the United States Department of Agriculture (USDA) is a multi- faceted agency that manages and protects 154 national forests and 20 grasslands in 44 states and Puerto Rico. The agency’s mission is to sustain the health, diversity, and productivity of the nation’s forests and grasslands to meet the needs of present and future generations.

NRE FS eSafety is the front end of Origami Risk eSafety which is a cloud-based Solution-as-a-Service. NRE FS eSafety is responsible for all data elements within OReS. The system has the ability to record and manage safety accidents/incidents. It provides the ability to collect the appropriate information on an incident or accident and route the necessary information through workflow events. The workflow events will collect the appropriate information needed to complete all required Office of Workers Compensation Program (OWCP) information for the Department of Labor. In addition, OReS provide the FS Office of Safety and Occupational Health (OSOH) visibility into the causes of accidents or incidents for reducing them in the future.

The users will log into the NRE FS eSafety by using GDCI ConnectHR.

This PIA is being created for the NRE FS eSafety which is a cloud-provided solution. This privacy impact assessment identifies how information about individuals is handled within NRE FS eSafety in accordance with OMB M-03-22.

# 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?**

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

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107

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.

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

Executive Order 12107, 12196, 12564, and 5 USC chapters 11, 33, and 63.

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

Yes:

- The Security Plan Status: Approved
- The Security Plan Status Date: 04/26/2024
- The Authorization Termination Date: 04/26/2027
- The Risk Review Completion Date: 10/01/2025
- The FIPS 199 classification of the system (MODERATE)

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

DOL/GOVT 1; OCFO NFC -1; OPM GOVT-1; OPM GOVT-10

**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
- Driver's License Number
- Passport Number
- License Plate Number
- Registration Number
- File or Case ID Number
- Student ID Number
- Employee Identification Number
- Department of Defense Identification Number
- Professional License Number
- Taxpayer Identification Number
- Business Taxpayer Identification Number (Sole Proprietor)
- Credit or 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 Phone Number
- Health Plan Beneficiary Number
- Business Mobile Phone Number (Sole Proprietor)
- Department of Defense Benefits Number

**Biographical Information**

- Name (Including Nicknames)
- Business Mailing Address (Sole Proprietor)
- Date of Birth
- Ethnicity
- Business Phone or Fax Number (Sole Proprietor)
- Country of Birth
- City or County of Birth

- Group or Organization Membership
- Religion or Religious Preference
- Citizenship
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Marital Status
- Spouse Information
- Child Information
- Military Service Information
- Race
- Nationality
- Personal Email Address
- Business Email Address
- Global Positioning System (GPS) or Location Data
- Employment Information
- Alias (Username or Screenname)
- Personal Financial Information (Including Loan Information)
- Business Financial Information (Including Loan Information)

**Biometrics**

- Fingerprints
- Hair Color
- DNA Sample or Profile
- Retina or Iris Scans
- Video Recording

**Distinguishing Features**

- Palm Prints
- Eye Color
- Signatures
- Dental Profile
- Photo

**Characteristics**

- Vascular Scans
- Height
- Weight
- Scars, Marks, or Tattoos
- Voice or Audio Recording

**Device Information**

- Device Settings or Preferences (e.g., Security Level, Sharing Options, or Ringtones)

- Cell Tower Records (e.g., Logs, User Location, or Time)
- Network Communication Data

**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
- Health Information
- Academic or Professional Background Information
- Civil or Criminal History Information/Police Record
- Case Files

Medical information required to with OWCP and/or OSOH regulations/requirements

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

NRE FS eSafety Information is integrated with the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, Paycheck8, OReS and The Forest Service Customer Relationship Manager (NRE FS CRM). If information is not readily available through data integration, the individual may be required to provide it only if it's deemed necessary to comply with OWCP and/or OSOH regulations/requirements.

**How is the information collected?**

NRE FS eSafety Information is integrated with the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, Paycheck8, OReS and NRE FS CRM. If information is not readily available through data integration, the individual may be required to provide it only if it's deemed necessary to comply with OWCP and/or OSOH regulations/requirements.

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

Not applicable

**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, which is the system of recording and will auto populate information automatically.

**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 though the use of third-party websites?**

Not applicable

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

**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: 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.**

NRE FS eSafety Information is integrated with the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, Paycheck8, OReS and NRE FS CRM. If information is not readily available through data integration, the individual may be required to provide it only if it's deemed necessary to comply with OWCP and/or OSOH regulations/requirements.

**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

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

**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

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

**How does the project, application, or 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.

**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.

**List the privacy risks and mitigations related to notice.**

**Privacy Risk**: There is an associated risk with the 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 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

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

**What information is retained and for how long?**

6730 Accident Reporting and Investigation Scheduled, Temporary (3 years after case closed), GRS 5.6, item 100 (DAA-GRS-2017-0006-0013)

6180 Insurance and Annuities Personal Injury records not forwarded to the Department of Labor Scheduled, destroy 15 years after compensation ceases or when deadline for filing a claim has passed, GRS 2.4 Item 101 (DAA-GRS-2016-0015-0013)

6720 Occupational Health, Occupational Health OSOH – Regulated Substance Monitoring and Exposure Records Schedule, 30-year Cut-off: End of FY in which monitoring is conducted GRS 2.7, item 040 (DAA-GRS-2017-0010-0004)

**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.**

6730 Accident Reporting and Investigation Scheduled, Temporary (3 years after case closed), GRS 5.6, item 100 (DAA-GRS-2017-0006-0013)

6180 Insurance and Annuities Personal Injury records not forwarded to the Department of Labor Scheduled, destroy 15 years after compensation ceases or when deadline for filing a claim has passed, GRS 2.4 Item 101 (DAA-GRS-2016-0015-0013)

6720 Occupational Health, Occupational Health OSOH – Regulated Substance Monitoring and Exposure Records Schedule, 30-year Cut-off: End of FY in which monitoring is conducted GRS 2.7, item 040 (DAA-GRS-2017-0010-0004)

**List the privacy risks and mitigations related to data retention.**

**Privacy Risk**: The risk associated with retention of information being retained longer than necessary. NRE FS eSafety 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. NRE FS eSafety aligns with NARA 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?**

NRE FS eSafety Information is integrated with the following internal USDA systems NFC Mainframe (BEAR/102), USDA EmpowHR, Paycheck8, OReS and NRE FS CRM. If information is not readily available through data integration, the individual may be required to provide it only if it's deemed necessary to comply with OWCP and/or OSOH regulations/requirements.

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

**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.

**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?**

The Forest Service Human Recourse Workers Compensation (FS HR WC) staff uses the U.S. Department of Labor's web system, eCOMP (Employees' Compensation Operations & Management Portal), allows the FS to file, manage, track, upload mandatory forms, and medical documents for workers' compensation claims.

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

**Privacy Risk**: Privacy risks associated with external sharing and disclosure include Unauthorized Access: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

**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. Due Diligence: Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.

# 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?**

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 Departmental Administration website.

**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 on 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 Departmental Administration website.

**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 Departmental Administration website.

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

Not Applicable

**List the privacy risks and mitigations related to redress.**

**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 Office/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

These questions describe technical safeguards and security measures:

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

PII is encrypted in NRE FS eSafety, access controls are in place to ensure only need-to-know individuals have access, and all users must authenticate through USDA ICAM Shared Services through ConnectHR to access NRE FS eSafety and can only access information base on role membership.

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

Each user in NRE FS eSafety 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.

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

There are no significant risks associated with the internal sharing of PII data. All personnel accessing NRE FS eSafety 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.

**Describe what privacy training is provided to users either generally or specifically relevant to the project, application, or system.**

All NRE FS eSafety users receive annual security awareness training that includes specific training regarding the protection of PII. Privileged users within NRE FS eSafety are required to take additional, more detailed security training commensurate with their access permissions. All training material and release dates are maintained and controlled by USDA.