Privacy Impact Assessment

for

NRE Forest Service eSafety (NRE FS eSafety)

Policy, E-Government and Fair Information Practices

Version: 1.0

Date: April 12, 2023

Prepared for: USDA FS Cybersecurity

Contact Point

Laree S. Edgecombe

System Owner

USDA NRE Forest Service

703-605-0820

Reviewing Official

Cynthia Ebersohn

Privacy Officer

USDA NRE Forest Service

386-301-4060

Abstract

NRE Forest Service eSafety (NRE FS eSafety) is the front-end system to Origami Risk eSafety (OReS). NRE FS eSafety is responsible for all data elements within OReS. The NRE FS eSafety uses ICAM Shared Service (formally known as eAuthentication) to access the system. A non-Forest Service employee will use a web browser to manually enter required data into NRE FS eSafety. An end user accessing eSafety through ICAM Shared Service will have their information prepopulated. Administratively Determined (AD) employees will use a web browser to enter all information and will receive update on their case via contacting the Human Resource Contact Center 1-877-372-7248.

NRE FS eSafety consists of the end user data maintained in Origami Risk eSafety as well as the controls to limit access and safeguard the data. All hardware and software associated with the processing of information is outside the boundary of NRE FS eSafety. NRE FS eSafety is responsible for controls related to the usage of the Origami Risk eSafety service including the management of user access, permissions, and application security configurations. 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.

NRE FS eSafety is not used by the public.

FISMA Children and / or Components

NRE FS eSafety inherits most technical controls from OReS. There are no subordinate child systems or component modules within NRE FS eSafety.

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 provides FS Office of Safety and Occupational Health 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. The URL is https://usdafs.connecthr.com/Login.

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 1.0 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?

NRE FS eSafety collects full name, date of birth, full address, email, social security number, driver's license number, unique identification number, health data, photographic images, Workers' Compensation and indemnity benefits information, information related to insurance policies and insured individuals and locations, insurance related data (i.e. insurance claim details, incident details, claimant information, witness information, litigation information and contacts, claim financial history), collect exposure values related to insurance exposures like safety systems, natural disaster exposure and other types of risks.

1.2 Source

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

Information is collected from data collected directly from employees, Forest Service systems such as FS HR Support System (FS HRSS), Paycheck8, National Finance Center (NFC) and Customer relationship management (CRM). Additionally, information provided by the Department of Labor (DOL) is also be used and collected.

1.3 Justification

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

This information is used to analyze and adjudicate claims made by the employee. Safety and workers compensation staff within the FS uses the information to help develop safety programs to mitigate future incidents, injuries and manage the Workers' Compensation claim. Data is transmitted electronically to the DOL to process claims.

1.4 Collection

How is the information collected?

General claim information is collected directly from the employee or someone completing the claim on their behalf. In addition, system interfaces provide data used to complete the claim for the DOL and sent via electronic interfaces.

1.5 Validation

How will the information be checked for accuracy?

NRE FS eSafety receives the NFC Bi-Weekly Examination Analysis and Reporting System (BEAR) data file feed on a biweekly basis which is the Human Resource database of record. Data can also be presented to NRE FS eSafety system via manual entry, data imports, and data conversion and update. Integrity checks within the system validate the data and generate error reports for application administrator review and remediation.

1.6 Authority

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

The legal authority to do so comes from Federal Employees Compensation Act (FECA) also known as 5 U.S.C. 8101 et seq. OMB M-17-12 (Preparing for and responding to a Breach of Personally Identifiable Information)

1.7 Risk Mitigation

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

NRE FS eSafety collects sensitive information that must be protected from breach. NRE FS eSafety utilizes multiple strategies in order to mitigate this risk. From the networking and transport level, eSafety utilizes firewalls, intrusion detection system (IDS)/intrusion prevention solution (IPS) software, and virtual private networks (VPNs) in order to minimize the network exposure of our systems. NRE FS eSafety encrypts all data in transit and at rest within the system. On the OS level, NRE FS eSafety employs a least privilege approach to providing access to servers as well as conducting audits and logging of security information. All access to NRE FS eSafety by users is conducted over encrypted SSL connections.

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.

The information collected is used to determine eligibility and the amount of benefits payable under the Federal Employees' Compensation Act (FECA). Information is also used to check status of claims, verify billing, and to consider issues relating to retention, rehire, rehabilitation, return-to-work programs/services or other relevant matters. The data can be used for treatment, medical, vocational rehabilitation, and for other purposes related to the medical management of the claim. The information can be used for litigation purposes as well.

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 Department of Labor

• 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

2.2 Analysis and Production

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

NRE FS eSafety utilizes analytic tools for describing the Risk Data kept in the system in order to understand insurance data and explore opportunities for cost saving. NRE FS eSafety back-end OReS utilizes Fusion Charts to produce dashboards and Logi XML to produce reports.

2.3 Commercial/Public Use

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

The system does not use commercial or publicly available data.

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.

Not Applicable.

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?

NRE FS eSafety data is retained for the lifetime of the contract between Origami Risk eSafety and the USDA Forest Service. Any archived data is retained indefinitely for litigation holds or Department of Labor claims. The NRE FS eSafety team is working with Chris Meadows on retention requirements with NARA.

3.2 Approval

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

These documents should be maintained apart from the Employee Medical Folder or OPF, but such folders are not considered a “system of records” separate from the case file. Rather, they are considered an alternate location for the records, which remain under the jurisdiction of the OWCP. Their retention and disposal is covered by the OWCP Records Retirement Schedule, which mandates that case file material should be maintained for two years after case closure.

3.3 Risk Mitigation

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

Origami often retains years of data to support historical analytics and the lifetime of ongoing insurance claims. Risk is mitigated through defense in depth (infrastructure), data encryption (AES-256), secure transmission protocols (SSL,TLS), Role-Based Access Controls (RBAC), input validation, and end user training.

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?

Not applicable.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Not applicable.

4.3 Risk Mitigation

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

Not applicable.

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?

The information gathered is collected from FS HR Support System (FS HRSS), Paycheck8, NFC, Customer Relationship Management (CRM), and data collected directly from employees which includes Personally Identifiable Information (PII), and/or financial information. This information is used to analyze and adjudicate claims made by the employee. Safety and workers comp staff within the FS use

the information to help develop safety programs to mitigate future losses and manage the workers comp claim. Department of Labor System, GDCI, Inc.; Used to determine eligibility for an employee the amount of benefits to be paid under the FECA for an OWCP claim.

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, provide SORN name and hyperlink URL to text.
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 collection and sharing of data is for the purpose of providing benefits to claimants. It is covered by the following SORN:

a. DOL/GOVT-1 - Office of Workers' Compensation Programs, Federal Employees' Compensation Act File

b. DOL/GOVT-1 addresses agencies right to maintain copies of records associated with a workers' compensation claim. In addition, it describes that agency copies fall under DOL's jurisdiction, and governs the retention and disposal of records. DOL/GOVT-1 can be reviewed at:
http://www.dol.gov/sol/privacy/dol-govt-1.htm

c. USDA OP-1 Personnel and Payroll System for USDA Employees
https://www.ocio.usda.gov/sites/default/files/docs/2012/OP%20-%201.txt

d. OPM GOVT-1 General Personnel Records
https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf

5.3 Delivery and Security Measures

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

Data is encrypted (in-transit, at-rest), using public keys and signatures, which can only be decrypted with the private key and transmitted across FTP channels using SSL. Information is secured by limiting access through role-based security, preventing users from accessing data they should not have access to. Additionally, any transmitted data uses SSL/TLS transmission protocols and encrypted using public/private keys.

5.4 Risk Mitigation

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

All external transmissions contain Personally Identifiable Information (PII), and/or financial information, thus requiring additional security resources. Risk is mitigated through defense in depth (infrastructure) approach, data encryption (AES-256), secure transmission protocols (SSL, TLS), Role-Based Access Controls (RBAC), input validation, and end user training.

Locked locations are used for paper files.

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?
If so, please provide SORN name and hyperlink URL to text.
If a SORN is not required, answer "No" to this question, and "N/A" for questions 6.2 through 6.5.

No. Department of Labor maintains the SORN, DOL-GOVT-1, USDA maintains the SORN USDA OP-1 Personnel and Payroll System for USDA Employees and OPM maintains the OPM GOVT-1 General Personnel Records

6.2 Individual Notification

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

Not applicable.

6.3 Right to Decline

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

Not applicable.

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?

Not applicable.

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.

Not applicable.

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?

Requests for access (from either the record subject or a third party) is described under the under the Freedom of Information Act. The message below will be provided in accordance with the Freedom of Information Act (FOIA) and USDA regulations at 7 CFR, any person can request access to USDA Forest Service (FS) records. The FOIA requires the FS to disclose records unless the information is exempt from mandatory disclosure under the FOIA (e.g., classified national security, business proprietary, personal privacy, investigative). Instructions on FOIA requests can be found on https://efoia-pal.usda.gov/

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Data is verified upon data entry into the system. Employees can contact the FS Human Resources (HR) to officially correct the inaccurate/erroneous data. Upon receipt of verification/validation of inaccurate/erroneous data, HR will correct the information into the appropriate NFC system. The established bi-direction feed will update NRE FS eSafety on a bi-weekly basis once a corrective data has been submitted and processed by NFC.

7.3 Notification

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

Requests for access (from either the record subject or a third party) is described under the under the Freedom of Information Act. The message below will be provided in accordance with the Freedom of Information Act (FOIA) and USDA regulations at 7 CFR, any person can request access to USDA Forest Service (FS) records. The FOIA requires the FS to disclose records unless the information is exempt from mandatory disclosure under the FOIA (e.g., classified national security, business proprietary, personal privacy, investigative). Instructions on FOIA requests can be found on https://efoia-pal.usda.gov/

7.4 Redress Alternatives

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

Specific materials in this system have been exempted from certain Privacy Act provisions regarding the amendment of records. The section of this notice entitled "Systems exempted from certain provisions of the Act," indicates the kind of materials exempted, and the reasons for exempting them. Any individual requesting amendment of non-exempt records should contact the appropriate OWCP district office, or the system manager. Individuals requesting amendment of records must comply with the Department's Privacy Act regulations at 29 CFR 71.1 and 71.9, and with the regulations found at 20 CFR 10.12.

7.5 Risk Mitigation

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

Personal Identifiable Information (PII), is collected in order to adjudicate claim and compensate the employee for injuries or illnesses sustained while on the job. This information is stored in an Encrypted database and only registered users with the proper security roles will have access to the information within eSafety. When information is transmitted to outside sources, such as the DOL the data will be encrypted and sent through secure channels. Risk is mitigated through defense in depth (infrastructure), data encryption (AES-256), secure transmission protocols (SSL, TLS), Role-Based Access Controls (RBAC), input validation, and end user training. Locked locations are used for paper file.

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?

The system is integrated with the USDA ICAM Shared Services (formally known as eAuthentication). Authentication for the ICAM Shared Services is managed at the USDA enterprise level. An ICAM Shared Service account consists of LincPass card or a User ID, a password and the customer's profile which contains information that will permit USDA applications to identify if the person has the correct permissions for access. Homeland Security Presidential Directive 12 (HSPD-12) mandates that federal agencies screen employees and contractors and issue credentials – or smartcards – that meet National Institute of Standards and Technology (NIST) guidelines. LincPass is the USDA smartcard. Using LincPass improves the security of the network and supported information systems in compliance with Federal Information Processing Standard (FIPS) 199.

8.2 Contractor Access

Will Department contractors have access to the system?

Yes.

8.3 Privacy Training

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

Information Security Awareness (ISA) training is Mandatory for all users.

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).

Yes. November 19, 2024

8.5 Audit and Technical Safeguards

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

Each authentication, authorization, and validation activity is logged by the ICAM Shared Services (formally known as eAuthentication). Successful and unsuccessful logins beyond specific thresholds are reported and reviewed on a daily basis to USDA ICAM Services.

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?

This information is stored in an Encrypted database and only registered users with the proper security roles will have access to the information within eSafety. When information is transmitted to outside sources, such as the DOL the data will be encrypted and sent through secure channels. Risk is mitigated through defense in depth (infrastructure), data encryption (AES-256), secure transmission protocols (SSL, TLS), Role-Based Access Controls (RBAC), input validation, and end user training. Locked locations are used for paper files.

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?

NRE FS eSafety is the front end of OReS. OReS is a Software as a Service (SaaS) Risk Management Information System, hosted on the Amazon Web Services (AWS) GovCloud and offered as a web application, accessed through a user's web browser. eSafety is built on a Microsoft technology stack, using Microsoft Windows OS, Microsoft Internet Information Services, ASP.Net and Microsoft SQL Server.

9.2 Privacy Concerns

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

No.

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?

Not applicable.

10.3 PII Availability

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

Not applicable.

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?

Not applicable.

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?

Not applicable.

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?

Not applicable.

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?

Not applicable.

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?

Not applicable.

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)?

Not applicable.

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?

Not applicable.

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?

Not applicable.

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.

Not applicable.

Responsible Official

CHARLES BARCLAY
Digitally signed by CHARLES BARCLAY
Date: 2023.09.14 11:13:38 -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: 2023.09.18 07:37:08 -05'00'

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

BENJAMIN MOREAU
Digitally signed by BENJAMIN MOREAU
Date: 2023.09.19 10:29:28 -04'00'

Benjamin Moreau
Assistant Chief Information Security Officer (ACISO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture