Privacy Impact Assessment

for

NRE FS Casepoint (NRE FS Case)

Policy, E-Government and Fair Information Practices

Version: 1.0

Date: January 18, 2023

Prepared for: USDA Forest Service – CIO Internal Controls - Privacy

Contact Point

Zahid Chaudhry

System Owner

USDA NRE Forest Service

503-808-2440

Reviewing Official

Cynthia Ebersohn

Privacy Officer

USDA NRE Forest Service

386-301-4060

Abstract

This Privacy Impact Assessment (PIA) addresses the USDA Natural Resources and Environment (NRE), Forest Service (FS), Casepoint (NRE FS Case) information system. NRE FS Case is a cloud-based e-discovery solution that provides a capability for secure cloud storage, sharing, and collaboration of USDA case data to support the Forest Service (FS) Litigation and Forensics Services eDiscovery program. Based on the Privacy Threshold Analysis (PTA), it was determined that NRE FS Case may store PII from a wide variety of federal and nonfederal entities, to include state and local government employees, university partners, short term (seasonal) contractors and researchers and that a PIA needed to be completed.

Overview

NRE FS Case is owned by the Forest Service, an agency under the United States Department of Agriculture (USDA). The system is used to support the Forest Service Litigation and Forensics Services eDiscovery Team in the delivery of its services to its customers.

NRE FS Case is a cloud-based content management solution. The solution is a tool used by the FS Litigation and Forensics Services eDiscovery Team and the customers they serve in providing expertise for criminal, Human Resources (HR), Freedom of Information Act (FOIA), and civil cases across the FS. NRE FS Case provides a general data repository that allows users to store content and collaborate from an organized, managed, and secure environment. The solution allows users to efficiently and responsibly: retain, categorize, find, manage, group, share, tag, cull, and dispose of USDA managed data processed by the system. The data mainly consists of documents, photos, videos, and audio recordings.

NRE FS Case utilizes Casepoint Government (CG), a cloud-based Software as a Service (SaaS) offering provided by Casepoint. CG is a FedRAMP authorized information system that allows for secure cloud storage, sharing, and collaboration. CG provides the FS with the capabilities needed to manage data in litigations, investigations, and FOIA requests. All data is subject to the organization’s policies in place to govern this data, to include privacy and organization-level security.

NRE FS Case is accessed by its users via the internet by going to the URL provided by CG.

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.

Identification

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

The information temporarily stored within NRE FS Case includes information involving criminal, administrative, FOIA, and civil cases. NRE FS Case is not a system of record and does not collect information from users. The information temporarily stored within NRE FS Case will have origins in other systems. NRE FS Case may contain Controlled Unclassified Information (CUI) and may inadvertently store PII such as name, address, email address, date of birth, SSN, TIN, etc., but does not collect PII directly from its users. In the event PII is identified in a data set it is redacted and annotated as redacted. CUI includes files that may include information relating to privacy, law enforcement, legal, safety, and security.

Source

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

The information temporarily stored within NRE FS Case is provided by the customers supported by the FS Litigation and Forensics Services eDiscovery Team and the sources include the following:

USDA employees.

• Contractors or other entities working on behalf of USDA.

• Non-USDA Federal Government employees.

• USDA Partner

• Other. (Benefactors, program participants, stakeholders, i.e. farmers, ranchers, producers, etc., these are still members of the public however, they have a degree of specific interest).

- State and Local Government Employees
- University Partners

- Short Term Contractors (Seasonal Workers)
- Researchers

Justification

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

NRE FS Case provides a capability that allows the FS Litigation and Forensics Services eDiscovery Team and the customers it supports to temporarily store and collaborate on information involving criminal, administrative, FOIA, and civil cases. The information is processed, reviewed, analyzed, and culled to produce a final product meeting the customers' needs related to their case/matter.

Collection

How is the information collected?

NRE FS Case does not collect information. The information temporarily stored within is provided by customers that are supported by the FS Litigation and Forensics Services eDiscovery Team. The information temporarily stored in NRE FS Case will be uploaded by users (System Administrators) via the Casepoint web-based application or desktop client tool.

Validation

How will the information be checked for accuracy?

Validation of information stored within NRE FS Case is the responsibility of the customer and their collaborator(s). Accuracy of information is to be confirmed prior to placing information in the system.

Authority

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

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

For additional Federal requirements for the collection of information, also see: 5 U.S.C. Chapter 552, 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management), and 18 U.S.C. 2071, 44 U.S.C. 3101 et seq., 44 U.S.C. 3506, Title 7 CFR 2.37, 36 CFR Chapter 12, Subchapter B, 36 CFR Part 1234, E-Government Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch. 36), OMB Circular - Disposition of Federal Records: A Records Management Handbook, NARA General Records Schedules.

Risk Mitigation

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

NRE FS Case does not collect data, however it is possible that content stored within NRE FS Case could contain PII, including SSN/TIN. In the event, PII is identified in a data set it is redacted and annotated as redacted. The information stored in NRE FS Case is protected through various levels of security and policy. Encryption is used to protect Information in transit and while at rest. Information is organized at the case/matter level and access to the system is limited to authorized users that only have access to the information they have been authorized to access by the Customer Lead responsible for the case/matter. System access requires Two-Factor Authentication utilizing a user ID, password, and security code.

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 temporarily stored in NRE FS Case is used to create a final product for the customer that enables them to satisfy their needs as it pertains to deliverables required for litigations, investigations, and FOIA requests. Customers and their collaborators will use the system to process, review, analyze, and cull their case/matter related information based on their requirements related to the case/matter.

2.2 Analysis and Production

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

NRE FS Case utilizes the tools available within the CG SaaS offering including advanced analytics and search tools to facilitate the review, analysis, and culling of the customer's information to meet their specific needs related to the case/matter. NRE FS Case does not produce any data other than ancillary data to understand the usage of the application and for audit trail purposes. The CG SaaS offering provides monitoring and auditing tools to produce the following reports:

- Usage reports
- User Statistics
- Folders and Files
- Collaborators
- Security Reports

Reports are provided in the form of Microsoft Office (Word, Excel, PowerPoint) documents that may be used to analyze the data from those reports.

2.3 Commercial/Public Use

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

Not Applicable - 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.

This content is protected through various levels of security and policy. The system itself is protected by access layers and positive identification techniques to ensure that only people authorized to view and act upon information can do so. User roles are outlined within the NRE FS Case Roles Responsibilities and Least Privilege Table. Privileged accounts are created by Casepoint Government and are restricted to members of the FS Litigation and Forensics Services eDiscovery Team. System access requires Two-Factor Authentication utilizing a user ID, password, and security code.

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 Case only temporarily stores information. The system is a general data repository that allows users to store and collaborate on information from an organized, managed, and secure environment. This allows the customer to gather and prepare information in a manner that is suitable to their needs related to their case/matter. Once the information is prepared and the final product is produced, the information is removed from the system.

The agency records officer (William Meadows) was consulted regarding a records retention schedule for the system, and it was determined that this system does not meet the definition of an official Agency record and therefore does not need to be assigned records retention schedule.

3.2 Approval

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

Not applicable - NRE FS Case only temporary stores data and does not need to be assigned a records retention schedule.

3.3 Risk Mitigation

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

NRE FS Case will only temporarily store data and is not the data source or system of record. The data will be removed once the customer data is processed, and the final product related to their case/matter is produced.

Overall, the risks are minimal as the system is implemented in accordance with USDA & FS policies and guideline and the SaaS offering utilized is a FedRAMP authorized solution.

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?

The USDA Office of the General Counsel (OGC) provides legal services for all programs, operations, and activities of USDA. OGC personnel providing support will have access to the system and information related to the case/matter they are supporting to facilitate the necessary collaboration and production of a consolidated case file.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Information is available to the OGC through the application and is not transmitted.

4.3 Risk Mitigation

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

The information available to the OGC is for official purposes and is directly related to the case/matter they are providing support for. The information is protected through various levels of security and policy and access control ensures that personnel only have access to the information that they are authorized to have access to.

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?

NRE FS Case does not directly share information with any external organizations. NRE FS Case is used to produce a final product based on the customers' needs related to their case/matter. The customer would be responsible for any distribution of their information contained within their final product. E.g. a customer supporting a legal matter would upload a consolidated case file to the Department of Justice.

The information may include, but is not limited to:

• Documents

• Photos

• Audio

• Videos

• Metadata defining all of the above.

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.

Not applicable – NRE FS Case is a temporary repository of data and is not the source or system of record. Information temporarily stored in the system is not accessible via indexing and cannot be retrieved by name or other personally unique identifier.

5.3 Delivery and Security Measures

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

NRE FS Case does not directly share or transmit information. NRE FS Case is used to produce a final product based on the customers' needs related to their case/matter. The customer would be responsible for any distribution of their information contained within their final product. NRE FS Case content is not

accessed from outside the department and only authorized individuals that have a need to know will receive access through the designated process.

5.4 Risk Mitigation

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

NRE FS Case does not directly share or transmit information outside the USDA.

Overall, the risks are minimal as the system is implemented in accordance with USDA & FS policies and guidelines and the SaaS offering utilized is a FedRAMP authorized solution.

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, NRE FS Case is a temporary repository of data and is not the source or system of record. Information temporarily stored in the system is not accessible via indexing and cannot be retrieved by name or other personally unique identifier.

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?

Not applicable - There are no procedures or use cases that apply to allowing individuals to gain access to their information. There is no way to search for information on any individual in the system.

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Not applicable - There are no procedures or use cases that apply to the correction of inaccurate or erroneous information. Any correction to data stored within NRE FS Case would be done in the system of origin.

7.3 Notification

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

Not applicable - There are no procedures or use cases that apply to individuals correcting their information. NRE FS Case is not a data collection tool or a system of record and does not have the capability to provide notice to individuals. Any correction would take place in the system of origin.

7.4 Redress Alternatives

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

Not applicable - Any redress available to individuals pertaining to any data within NRE FS Case would only be applicable to and take place within the system of origin.

7.5 Risk Mitigation

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

Not applicable - NRE FS Case is not a data collection tool or a system of record. Any redress available to individuals pertaining to any data within NRE FS Case would only be applicable to and take place within the system of origin.

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?

All organizational users must fill out an access request form that is elevated to the NRE FS Case System Administrators for access to the system. Once the account is created the NRE FS Case System Administrators will grant the user the appropriate level of access.

8.2 Contractor Access

Will Department contractors have access to the system?

No

8.3 Privacy Training

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

All USDA personnel are required to complete annual Department Information Security Awareness training. The interactive online training covers topics such as properly handling Sensitive PII and other data, online threats, social engineering, and the physical security of documents and electronics, such as laptops and mobile devices. Individuals with significant security responsibilities (such as Administrators) are required to undergo additional role-based training, tailored to their respective responsibilities.

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, the current ATO expires 2/23/2024.

8.5 Audit and Technical Safeguards

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

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, Rev. 5. This includes at a minimum:

• User identification and authentication

• The use of network and application access controls

• Encryption of data at rest, in transit, and in use

• Auditing of significant changes to systems or data.

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?

NRE FS Case does not collect data. The information temporarily stored in NRE FS Case is subject to confidentiality and integrity related risks while in transit and at rest.

Information stored within NRE FS Case is protected in transit utilizing Transport Layer Security (TLS) 1.2 protecting the confidentiality and integrity of the information. Protection for information at rest is accomplished through access control and encryption. NRE FS Case eliminates exposure of data transmittal, as data is not transmitted. Files stored in NRE FS Case are encrypted while at rest or in use in compliance with FIPS 140-2 validated cryptography.

NRE FS Case will promptly report computer security incidents and breaches affecting USDA data/information or systems and promptly coordinate with FS staff on incident handling, response, containment, eradication, and recovery efforts throughout the incident life cycle until fully resolved.

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?

System

9.2 Privacy Concerns

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

No, none of the technology used raises privacy concerns. The technology employed consists of a FedRAMP authorized SaaS offering. The temporary storage of data in the system while being processed may contain PII. In the event PII is identified in a data set it is redacted and annotated as redacted. Information temporarily stored in NRE FS Case is subject to confidentiality and integrity related risks while in transit and at rest.

Information stored within NRE FS Case is protected in transit utilizing Transport Layer Security (TLS) 1.2 protecting the confidentiality and integrity of the information. Protection for information at rest is accomplished through access control and encryption. NRE FS Case eliminates exposure of data transmittal, as data is not transmitted. Files stored in NRE FS Case are encrypted while at rest or in use in compliance with FIPS 140-2 validated cryptography.

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 - NRE FS Case does not use third party websites and/or applications.

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 - NRE FS Case does not use third party websites and/or applications.

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 - NRE FS Case does not use third party websites and/or applications.

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 - NRE FS Case does not use third party websites and/or applications.

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 - NRE FS Case does not use third party websites and/or applications.

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 - NRE FS Case does not use third party websites and/or applications.

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 - NRE FS Case does not use third party websites and/or applications.

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 - NRE FS Case does not use third party websites and/or applications.

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 – NRE FS Case does not use Web measurement and customization technology.

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 - NRE FS Case does not use Web measurement and customization technology.

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 - NRE FS Case does not use third party websites and/or applications.

Responsible Official

ZAHID CHAUDHRY
Digitally signed by ZAHID CHAUDHRY
Date: 2023.05.30 10:24:15 -07'00'

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

Approval Signature

CYNTHIA TOWERS
Digitally signed by CYNTHIA TOWERS
Date: 2023.05.31 09:01:36 -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: 2023.06.10 21:50:29 -04'00'

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