Privacy Impact Assessment

for

Pinyon

Policy, E-Government and Fair Information Practices

Version: 1.2

Date: 5/28/2023

Prepared for: USDA FS CIO

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

Pinyon is a US Forest Service enterprise implementation of a new agency wide repository with the capabilities of managing documents and digital assets (photos, videos & audios) for the agency.

Pinyon is a cloud-based solution offering with the following capabilities: Electronic Document Management; Enterprise File Sync and Share (internal FS and external partners and other agencies); Digital Asset Management (photo, video, audio); Electronic Records management; and Support eDiscovery/Litigation Hold capabilities.

Based on the Privacy Threshold Analysis (PTA), it was determined that Pinyon stores 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

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.

Pinyon is an enterprise content management (ECM) cloud-based solution as a service. PINYON is a Cloud Service. PINYON is hosted by Box, Inc, which has a FedRAMP ATO that is separate. Box FedRAMP is managed by the USDA OCIO ISC. and has its own separate instance.

The purpose is to provide a document and digital asset management repository for the agency. Pinyon provides the capability to manage electronic and physical records in accordance with National Archives and Records Administration (NARA) guidelines across the enterprise in multiple repositories, using a federated approach. The ECM solution will allow users to efficiently and responsibly: retain, categorize, find, manage, group, share, tag and dispose of FS content in the form of documents, photos, videos & audios.

Users log into Pinyon by going to a URL on the web from within US Forest Service Network or from the public Internet.

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?

The types of content that are stored, used, disseminated, and maintained are types defined in the System Categorization. Pinyon is a content management system in support of the USDA Forest Service mission. Data stored may contain information from several agencies and/or organizations in support of the USDA Forest Service mission. Pinyon is a moderate system and contains both non-sensitive (public releasable) and controlled unclassified information (CUI). The data may contain PII however Pinyon does not collect PII directly from its users. Potential PII found in the data can be found on OMB 17-12, Data Elements and Information Type.

1.2 Source

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

Sources for the content contained within Pinyon include:

- USDA employees.
- Contractors or other entities working on behalf of USDA.
- Non-USDA Federal Government employees.
- USDA Partner
- Other
    - State and Local Government Employees
    - University Partners
    - Short Term Contractors (Seasonal Workers)
    - Researchers

Pinyon is not an information collection system where users enter data for collection purposes.

1.3 Justification

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

Pinyon's customers are responsible for managing the collection, use, dissemination and maintenance of information they store in the Pinyon content management system in accordance with the SORNs and record schedules associated with the content they store.

1.4 Collection

How is the information collected?

Pinyon is a content management system; information is not directly collected by the end user. The content is stored by the end users via web-based apps, desktop clients and mobile apps.

1.5 Validation

How will the information be checked for accuracy?

Information is not directly collected by Pinyon; it is the responsibility of the submitter/uploader and the collaborator(s) to confirm the accuracy of the information prior to placing information in Pinyon.

1.6 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 A-130, NARA - Disposition of Federal Records: A Records Management Handbook, NARA General Records Schedules.

1.7 Risk Mitigation

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

Pinyon is a content management system that does not directly collect data; however, it is possible that content stored within Pinyon could contain PII, including SSN/TIN. This content is protected through various levels of security and policy. All users accessing Pinyon must authenticate to the system prior to accessing data. The system itself is protected by access layers and data is marked to ensure that it is easily identified and that only people authorized to view information can do so. Users gain access when data custodians grant permissions to the data that they manage. Encryption is used to protect data at rest and in transit.

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.

Pinyon is used for file storage and collaboration of work products between authorized individuals. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside FS as a routine use pursuant to 5 U.S.C. 552a(b)(3).

2.2 Analysis and Production

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

Pinyon is a content management system and thus does not produce any data other than ancillary data to understand the usage of the application and for audit trail purposes.

Pinyon System will provide monitoring and auditing tools to produce the following reports

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

Security 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. Data is marked to signify if it is CUI so that data custodians are aware of special handling requirements. User roles are outlined within the Pinyon User Appx A Roles, Responsibilities, and Least Privilege Table.docx. Organizational user accounts are created and authenticated through the USDA ICAM Shared Services, formally known as eAuthentication.

Content Custodians are responsible and accountable to assign appropriate “need to know” permissions to other users to edit, view, or preview their managed content.
Pinyon will deploy the use of the standard ‘Box Classification’ capability in Pinyon to provide an extra layer of security on CUI content. Box Classification capability includes the ability for content custodians to apply ‘CUI’ visual indicators whereby they can see that a document/folder is marked as CUI. It also provides a customized advisory message on mouse over to allow users to see how to treat this type of content. CUI classification will also provide the controls to restrict sharing the link of CUI content beyond current permissions. From a usability standpoint it provides an easy method for users to clearly identify content with CUI and the ability to search for CUI content by classification type. Only users who are granted appropriate access to manage and see CUI content are able to retrieve search results by CUI classification type. Search results are only displayed based on the user’s access to content.

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?

- All information contained will be retained in compliance with NARA Guidelines, which vary from five to ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017.

- Individuals have control of the shelf life for retention. If the user leaves, their account gets disabled.

3.2 Approval

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

Yes.

3.3 Risk Mitigation

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

The risks associated with the retention time is in accordance with the FS Records Management Policy

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archive and Records Administration (NARA). (DR 3080-1 Records Disposition http://www.ocio.usda.gov/records/policy.html).

The disposition instructions in mission area, agency or staff office record schedules are mandatory. Officials may not dispose of records prior to their authorized disposal date or retain them beyond that date except in situations in which records might be relevant to pending or threatened litigation. If a program official determines that records need to be retained longer than authorized by the schedule, the mission area, agency, or staff office records officer shall be contacted to obtain approval from NARA and, if necessary, to revise the schedule.

The actions taken regarding records and non-records no longer needed for current Government business include transfer to agency storage facilities or Federal records centers, transfer from one Federal agency to another, transfer of permanent records to the National Archives, and disposal of temporary records. For non-records, these actions include screening and destruction. Destruction is the primary type of disposal action and can include burning, shredding, deleting, or discarding with other waste materials. In the electronic realm, destruction is typically accomplished by overwriting or degaussing, depending on security requirements.

Section 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?

> PII information is stored within Pinyon and shared with authorized USDA employees, contractors, and affiliates with a need-to-know to conduct the business of the organization. Note, however, that this 'sharing' is a manual process of authorized users accessing the data files, and not an automated function of the Pinyon system/application.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

> Any 'shared' PII is the result of authorized USDA users accessing data files stored in Pinyon.

4.3 Risk Mitigation

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

> Privacy risks are mitigated by granting access through role-based authorization using USDA ICAM Shared Service (eAuthentication), and FIPS 140-2 certified encryption. Any residual risk is mitigated by the controls discussed in Section 2.4 above.

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?

> Pinyon's data stored and shared may contain information from several agencies and/or organizations in support of the USDA Forest Service mission. Externally information shared outside the Forest Service, or the Department of Agriculture may include Contractors or other entities working on behalf of USDA, Non-USDA Federal Government employees, USDA Partner, State and Local Government Employees, University Partners, and Researchers.

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 - The system does not collect information nor is the data base of record.

5.3 Delivery and Security Measures

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

> Access will be provided based on need to know, which will be safeguarded by a Role based authorization, eAuthentication and Box security mechanism.

5.4 Risk Mitigation

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

Privacy risks are mitigated by granting access through role-based authorization, USDA ICAM Shared Service (eAuthentication), Box login and FIPS 140-2 certified encryption. Any residual risk is mitigated by the controls discussed in Section 2.4 above.

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

6.2 Individual Notification

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

N/A

6.3 Right to Decline

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

N/A

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?

N/A

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.

N/A

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 - Pinyon is a content management system. There are no procedures 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 - Pinyon is an enterprise content management system that provides management and storage of data files only. Any correction to the data stored within Pinyon, would be done in the system of origin by the data owner.

7.3 Notification

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

> Not applicable - Pinyon is not a Data collection tool. It is a content data system that stores data and does not have the capability to provide notice to individuals.

7.4 Redress Alternatives

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

> N/A

7.5 Risk Mitigation

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

Not applicable - Pinyon is not a Data collection tool. It is a content management system that stores data.

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 use ICAM Shared Service (also known as eAuthentication) to access Pinyon. There is no formal approval process needed. All non-organizational users will be identified in the system by content custodians (sub-set of organizational users) based on the Data Sharing Agreement between Content Custodian/Business unit and the non- organizational user/partner. Content Custodians will request to collaborate with a non- organizational user via the Help Desk. System owner or designee (operations) will verify the request and request Pinyon Admin to create an external collaboration space with the right permissions and access.

Content Custodian is defined as an individual (or individuals) who have responsibilities within a functional area for FS information. They include unit line officers, file structure stewards, and/or content authors. For specific documents, they are the original creator or source for the information, and any other individual given the right/privilege to administer the data, including reading, sharing, deleting, and modifying. They are also defined as the persons who can select others with a need-to-know for read/view/modify of the PII data.

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?

All FS staff members are required to complete annual Department Information Security Awareness training which includes Rules of Behavior. The interactive online training covers topics such as properly handling 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).

Pinyon has completed Certification & Accreditation and has a current ATO expiring on 1/6/2026.

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.

Due to the public nature of this document, the method of encryption can be found in the Pinyon System Security Plan, control SC-13. All encryption is FIPS 140-02 compliant.

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?

Pinyon does not collect data; it is a content management system. PINYON provides security of content while at rest through the access methods and encryption. It eliminates exposure of data transmittal, (as data is not transmitted) but is accessed by a link which is sent via email. Files stored in Pinyon are encrypted while at rest, in transit, or in use in compliance with FIPS 140-2 validated cryptography. The method of encryption can be found in the Pinyon System Security Plan, control SC-13.

There is minimal risk to the user or named participants of the system. The mitigation of risk is handled by making sure that there is limited use and sharing of information, and only to relevant individuals.

Pinyon Solution as a Service will promptly report computer security incidents and breaches affecting FS data 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?

Major Application

9.2 Privacy Concerns

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

Pinyon's Content Custodians are responsible and accountable to assign appropriate "need to know" permissions to other users to edit, view, or preview their managed content. In addition, Pinyon will deploy the use of the standard 'Box Classification' capability in Pinyon to provide an extra layer of security on CUI content. Box Classification capability includes the ability for content custodians to apply 'CUI' visual indicators whereby they can see that a document/folder is marked as CUI. CUI classification will also provide the controls to restrict sharing the link of CUI content beyond current permissions.

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?

N/A

10.3 PII Availability

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

N/A

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?

N/A

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?

N/A

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?

N/A

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?

N/A

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?

N/A

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)?

N/A

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?

N/A

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?

N/A

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.

N/A

Responsible Official

ZAHID CHAUDHRY Digitally signed by ZAHID CHAUDHRY Date: 2023.06.20 12:10:51 -07'00'

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

Approval Signature

CYNTHIA TOWERS Digitally signed by CYNTHIA TOWERS Date: 2023.06.26 10:25:38 -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: 2023.06.27 16:13:25 -04'00'

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