

Privacy Impact Assessment for

Pinyon (Pinyon)

Policy, E-Government and Fair Information Practices

Version: 1.6

Date: October 10, 2019

Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)





Contact Point

Denise L. Burroughs

System Owner

USDA NRE Forest Service

202-699-1677

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

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 Software as a Service (SaaS) offering with the following capabilities: Simple, fast, reliable, & easily searchable repository; 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.

Forest Service Pinyon is an enterprise content management (ECM) cloud based solution as a service. The purpose is to provide a document and digital asset management repository for the agency. The solution will provide the capability to manage electronic and physical records as per 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 Forest Service content in the form of documents, photos, videos & audios.

Pinyon is a Software as a Service (SaaS) offering with the following capabilities:

Simple, fast, reliable, & easily searchable repository

Electronic Document Management

Enterprise File Sync and Share (internal FS and external partners and other agencies)



Digital Asset Management (photo, video, audio)

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

This PIA is being created for the FS Pinyon which is a cloud provided solution. This privacy impact assessment identifies how information about individuals is handled within Pinyon 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?

Pinyon is a content management system in support of the USDA Forest Service mission. Documentation will be stored that will contain information from several agencies/organizations in support of Forest Service mission. The types of content that will be stored, used, disseminated and maintained are types defined in the System Categorization. Pinyon is a moderate system and will contain both non-sensitive (public releasable) and controlled unclassified information (CUI). Pinyon may store PII but does not collect PII directly from its users. CUI includes files that may include information relating to Privacy, Financial, Law Enforcement, Legal, Safety, and Security.

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. (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

Pinyon is not a collection information system where users enter data for collection purposes. It is a file based storage and sharing platform for documents such as Word, PowerPoint, Portable Document Format (PDF), etc.

1.3 Justification

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

The principle purpose of storing files in FS Pinyon is to provide a repository for the information needed for supporting the USDA mission within the Forest Service Framework. Serving more as a general data repository, Pinyon will be used to allow USFS users to store and share work products in an organized, managed, and secure environment that will ensure confidentiality, integrity, and availability of Forest Service data.

1.4 Collection

How is the information collected?

The content in FS Pinyon System will be uploaded by users via web based apps, desktop clients and mobile apps.

1.5 Validation

How will the information be checked for accuracy?

Content is stored in Pinyon. It is the responsibility of the submitter 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 does not 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.

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.

FS 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?

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

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

Usage reports

User Statistics

Folders and Files

Collaborators

Security Reports

Microsoft Excel spreadsheets may be used to analyze the data from those reports. High level trend reporting may be produced within Microsoft PowerPoint or Word documents.

2.3 Commercial/Public Use

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

N/A. - 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 system *Roles, Responsibilities and Least Privilege Table*. Organizational user accounts are created and authenticated through the USDA eAuthentication SAML integration.

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 will provide 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 will be 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 official Agency Records shall be retained and maintained as per NARA approved records retention schedules and per direction found in FSH 6209.11 (FS Records Management Handbook).

In the absence of an updated, approved Records Retention Schedule/Disposition Authority, all records are to be considered permanent and must be retained accordingly until otherwise/appropriately scheduled and approved by NARA.

In the absence of the agency policy for non-records the information will be retained for 5 years.

3.2 Approval

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

All existing records retention schedules and retention periods are approved by the FS records management officer and NARA

3.3 Risk Mitigation

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

In the absence of an approved Records Retention Schedule/Disposition Authority, all records are to be considered permanent and must be retained accordingly until otherwise/appropriately scheduled and approved by NARA. In addition, the Agency must ensure that the existing locations and maintenance methods of this data comply with the applicable laws, regulations, authorities, and policies. Without this compliance, the Agency is subject to litigation, unable to perform mission critical activities, and more.

At an application level the ECM solution provides flexible control and audit features and granular asset level security for content at rest and in-motion at



the file level through content encryption with FIPS 140-2 across the IBM and Box joint solution. In addition, it will comply with Forest Service and US Department of Agriculture policies and guidelines. The solution will be based on platforms that have achieved FEDRAMP compliance

One of the risks is that the underline repository may become obsolete over time. To mitigate the risk the PINYON project includes an exit strategy.

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?

Content is accessible within US Forest Service, USDA and any other USDA participating agencies. Content is accessible for storage and collaboration to facilitate Forest Service day to day business securely, efficiently and effectively.

Content may include but is not limited to: Documents, Photos, Audio, Videos, and Metadata defining all content.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Pinyon does not transmit information. Content is stored in a secure location and is accessible by authorized individuals.

4.3 Risk Mitigation

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

Pinyon enterprise administration settings restrict access by requiring Admins and Content Custodians to invite authorized users to a folder or specific document. If the user has not been invited to collaborate by receiving a shared link they will not be able access content in Pinyon. A user can be invited to collaborate into a folder at one of seven access levels. It is possible to configure collaboration invites to allow users to view or submit content without allowing them to add other users or make changes.

Collaborations permissions can be upgraded, downgraded, or removed entirely by users who have the rights to change the access control list.



Only Content Custodians (owners and co-owners) of the folder will be allowed to invite collaborators into a folder. Requests to share content externally requires multiple levels of approvals, before content can be shared externally.

Overall the privacy risks are minimal as the system will be implemented in accordance to USDA & FS policies and guidelines. The solution will be based on platforms that have achieved FEDRAMP compliance.

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 content is accessible to the following, by invite only:

contractors or other entities working on behalf of USDA;

non-USDA Federal Government employees;

USDA Partner;

State and Local Government employees;

University Partners;

Short Term Contractors (Seasonal Workers);

Researchers; and

Others. (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);

Content is accessible for collaboration to facilitate Forest Service day to day business securely, efficiently and effectively.

Content may include but is not limited to: Documents, Photos, Audio, Videos, and Metadata defining all content.

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. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

N/A. - The system does not collect information. Files stored in Pinyon are 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?

Pinyon does not transmit information. It is a general data repository that allows USFS users to store and collaborate content from an organized, managed, and secure environment. Pinyon content is accessed from outside the department by those authorized individuals that have received explicit invites to collaborate in a workspace via a shared link

5.4 Risk Mitigation

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

The risks of privacy will be managed through a combination of people, processes and technology. A process will be in place to ensure organizational users have a Data Sharing Agreement in place before inviting non-organizational users to access any information in PINYON. It will be verified that organizational users has read, signed, and understands the required [Security Responsibility Form\(s\)](#)

External entities must have a valid Data Sharing Agreement in place prior to being permitted access to information on Pinyon. Data Sharing Agreements will be reviewed annually.

A centralized administrative process of managing external collaboration in Pinyon along with Box fine grained auditing capabilities will further mitigate the associated risks.

Overall the privacy risks are minimal, and Pinyon has been implemented in accordance to USDA & FS policies and guidelines. The solution is based on platforms that have achieved FEDRAMP compliance

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 and if so, please provide SORN name and URL?

(Note: 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?

N/A. Pinyon is a content management system and information access is controlled using roles and permission sets. 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?

N/A. Pinyon is an enterprise content management system that provides for the management and storage of information 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?

N/A. Pinyon is not a Data collection tool. It is a document repository 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.

N/A. Pinyon is not a Data collection tool. It is a document repository and does not have the capability to provide notice to individuals.



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 with eAuth assurance level 2 are pre-approved to access Pinyon Repository. 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 Customer Help Desk (CHD). 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 Forest Service information. They include unit line officers, file structure stewards, and/or content authors. For specific documents, they would be original creator or source for the information, and any other individual given the right/privilege to administer the data to include 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. 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).

Pinyon has completed Assessment & Authorization and the expiration date is January 7, 2020.

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. 4. 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; and

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?

Pinyon does not collect data; it is a content repository. 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/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?

Major Application

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?

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

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

Approval Signature

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

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture