Privacy Impact Assessment
FPAC Box

Policy, E-Government and Fair Information Practices

- Version: 2.2
- Date: February 19, 2021
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

FPAC Box

February 19 , 2021

Contact Point

Lisa Dieckmann
FPAC – BC
816-823-1597

Reviewing Official

James Flickinger
Chief Information Security Officer, FPAC
United States Department of Agriculture
(816) 926-6010

Abstract

FPAC Box is the name of the software component and system for this PIA. FPAC Box is a secure cloud-based, user-centric platform that enables government agencies to perform more efficiently by connecting public servants and constituents to their information. Users can upload documents and photos to a shared files folder, determine how their content can be shared with other users, and invite others to view and/or edit shared files. The PIA is being conducted due to PII information that may be contained within the documents transmitted or housed within the FPAC Box secure cloud environment.

A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101).

Overview

The United States Department of Agriculture Farm Production and Conservation (FPAC) Business Center has a number of legacy file storage repositories that have become either obsolete or costly to maintain. FPAC Box compliments secure file transfer, storage and archiving in a FedRAMP certified environment which utilizes encryption in transit and at rest. FPAC Box provides an ideal platform for cloud storage, allowing secure internal and external collaboration with partners and customers. The Box Enterprise Cloud Content Collaboration Platform is a FedRAMP certified SaaS solution.

- FPAC Box will provide the following capabilities: Unlimited Data Storage
- Robust access control and audit capabilities
- Share documents in real-time across the organizations securely and when needed;
- Improved security by eliminating the need for unsecure FTP servers
- Eliminates the need for physical shipment of data storage media.
- Provide secure mobile access to all data stored in the CFS solution
- Allow external customers to consume public information

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

FPAC Box contains documents stored in a file repository that may include a wide range of PII. Note: Any PII is stored on files that are uploaded and stored in FPAC Box. FPAC Box does not collect any information via data entry fields. The documents on FPAC Box are encrypted. Potential PII found in the documents includes (is estimated, but may not be limited to):

- Name
- Date and/or place of birth
- Address information (street or email address)
- Personal identification number (e.g. social security number, tax identification number, passport number, driver's license number or a unique identification number, etc.)
- Financial data
- Criminal history
- Employment history
- Photographic image
- Handwriting or an image of the signature
- Producer planning decisions and planning maps regarding private land management
- Miscellaneous information numbers (agency assigned number, case number, accounts, permits, etc.).

1.2 What are the sources of the information in the system?

- Information from the affected members of the public (i.e., farmers, landowners, etc.) may be entered in through FPAC Web applications, then is only manually stored in FPAC Box. FPAC Box does not process any financial transactions, and will never share any type of PII with any system.

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

- To support a collaborative environment amongst USDA employees, contractors, and affiliates within the confines of the SORN to accomplish mission needs

1.4 How is the information collected?

- The information ingested from various sources to include (documents, application, manual inputs, and records).

1.5 How will the information be checked for accuracy?

- FPAC Box does NOT directly collect PII information, instead information is derived from FPAC applications and stored in the FPAC Box Storage-as-a-Service infrastructure. Accuracy checks are performed by the personnel storing via the applications used to store data within FPAC Box.

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

- These regulations are applicable:
  - Privacy Act (5 U.S.C. §552a);
  - E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101);
  - Paperwork Reduction Act of 1995 (44 U.S.C. §3501)

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

- FPAC Box does **NOT** directly collect PII information, instead information is derived from FPAC applications and stored in FPAC Box.
- PII is stored on Box Inc. Storage-as-a-Service infrastructure. Risk is mitigated based on vendor's meeting FISMA, NIST and FedRAMP certifications.
- Privacy risks are mitigated because access to the information will be limited to appropriate FPAC personnel and partners by the use of the Role-Based model involving USDA e-Authentication, SSO, or domain credentials.
- Please see Section 2.4 and Section 8.6 for a further discussion of security controls that are in place to mitigate privacy risks.

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 Describe all the uses of information.

- For administration, FPAC Box uses the PII that was initially obtained from LDAP to establish the user's profile. FPAC Box can also be used to update the PII that is maintained for individual users, if they choose to modify their own profile.

- The PII within the data files will be used to support mission goals.

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

- PII is not "analyzed" by any tools. No PII data is "produced" by FPAC Box.

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

- FPAC Box can be used to disseminate public information such as documents, PDF forms, diagrams or announcement details.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

- This application is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.
- If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.
- The controls listed in this section shall be implemented in compliance with Federal and USDA standards regardless of deployment environment.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 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.
- Per the FPAC System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs".
- Individuals have control of the shelf life for retention. If the user leaves, their account gets disabled.

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

- Yes

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

- The primary risk is that a data breach could result in the inappropriate release of PII information related to FPAC Box user(s). This is mitigated via the use of role-based authorization, e-Authentication, and Digital Rights Managements (DRM), which includes FIPS 140-2 certified encryption.
- Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed above.

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 With which internal organization(s) is the information shared, what information is shared and for what purpose?

- PII information is stored within FPAC Box 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 FPAC Box system/application.

4.2 How is the information transmitted or disclosed?

- Any 'shared' PII is the result of authorized USDA users accessing data files stored in FPAC Box.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

- Privacy risk are mitigated by only transmitting information to authorized employees, contractors and affiliates with need-to-know based on role-based authorization, e-Authentication, and FIPS 140-2 certified encryption.
- Any residual risk are 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 With which external organization(s) is the information shared, what information is shared, and for what purpose?

- PII information is shared with FPAC employees, contractors, and partners when deemed required to complete assigned task.

5.2 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.

- The sharing of PII information with partners is compatible with the original collection, and is covered in the SORN.

5.3 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 and eAuthentication security mechanism.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

- Privacy risks are mitigated by preventing the release of PII to affiliates (farmers and landowners) through role-based authorization, e-Authentication, and FIPS 140-2 certified encryption.
- Any residual risk are mitigated by the controls discussed in Section 2.4 above.

Section 6.0 Notice

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 Does this system require a SORN and if so, please provide SORN name and URL.

- FPAC Box is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

- FPAC Box does NOT collect the PII information directly from the individuals

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

- Not applicable: FPAC Box does NOT collect the PII information directly from the individuals

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

- Not applicable: FPAC Box does NOT collect the PII information directly from the individuals

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

- There is no risk that any Landowner would be unaware of "collection," because FPAC Box does not directly collect information. FPAC Box is a storage drive.

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 What are the procedures that allow individuals to gain access to their information?

- FPAC Box does not directly collect PII from the individual. Individuals will gain access to their information via the Agency that owns the application that collects the information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

- FPAC Box does not directly collect PII from the individual. Individuals will gain access to their information via the Agency that owns the application that collects the information.

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

- FPAC Box does not directly collect PII from the individual. Individuals will gain access to their information via the Agency that owns the application that collects the information.

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

- FPAC Box does not directly collect PII from the individual. Individuals will gain access to their information via the Agency that owns the application that collects the information.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

- FPAC Box does not directly collect PII from the individual. Individuals will gain access to their information via the Agency that owns the application that collects the information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

- Access to this application is enforced via eAuthentication, RBAC, and DRM, which includes FIPS 140-2 certified encryption. User must have a valid "need to know" determined by requirements to perform applicable official duties. The system is in compliance with FISMA and USDA directives.

8.2 Will Department contractors have access to the system?

- Yes, authorized contractors and partners will have access to the system consistent with their roles and responsibilities. Access to FPAC Box is controlled through role-based authorization, eAuthentication, and DRM, which includes FIPS 140-2 certified encryption.

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

- Annual organizational Privacy Awareness Training is mandatory for all FPAC personnel. FPAC requires that every employee, contractor, and affiliate receives information security awareness training before being granted network and account access, per General Manual, Title 270, Part 409 - Logical Access Control and Account Management. Annual Security Awareness and Specialized Training is also required, per FISMA and USDA policy, and is tracked by USDA.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

- Authorization and Assessment is currently in process

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

- FPAC complies with the "Federal Information Security Modernization Act of 2014" (FISMA). Assessment and Accreditation, as well as annual key control self-assessments, and continuous monitoring procedures are implemented for this application per the requirements given in NIST SP 800-53. Additionally, FPAC complies with the specific security requirements for "auditing measures and technical safeguards" provided in OMB M-07-16. Finally, the system provides technical safeguards to prevent misuse of data including: o Confidentiality: Encryption is implemented to secure data at rest and in transit for this application (e.g., by FIPS 140-2 compliant HTTPS and end-user hard disk enc1yption). The documents that are passed to and maintained in FPAC Box are encrypted in transit.
    - Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth)
    - Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC). Administrative and management operational controls in place to ensure proper access termination.
    - Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
    - Audit: Logging is implemented end to end for this application (e.g. by logging infrastructure).
    - Attack Mitigation: The system implements security mechanisms such as input validation.

8.6 Privacy Impact Analysis: 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?

- FPAC Box is a third-party SaaS solution and does not directly collect any PII from any individual user, but does store PII from applications and documents.
- Privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5, and by the security controls discussed in Section 2.4 Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5 respectively.

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 What type of project is the program or system?

- FPAC Box is a SaaS which is an architecture model in which a provider provides file storage on their infrastructure, allowing internal/external file sharing ability, with an Authority to Operate (ATO).

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

- FPAC Box employs a file sharing technology which utilizes RBAC in their implementation

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 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 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

- FPAC Box APIs for application integration are the most inclusive to the current FPAC application infrastructure. Box provides the ideal Cloud platform within the FedRAMP certified realm for cloud storage allowing internal / external collaboration from partners and customers

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

- The third-party solution can only be accessed through USDA Role-based security controls.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

- The PII that becomes available through the agency's use of third-party applications utilize FIPS 140-2 encryption for storing, transmitting, and decrypting information at endpoints.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

- Any PII that becomes available through the agency's use of third-party applications will be maintained and secured by the vendor, Box Inc.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

- No

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

- USDA employees and contractors

10.8 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?

- PII via the agency's use of third-party applications will be shared with the partners for which that information was intended for – either internally or externally.

10.9 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)?

- No, the systems storage of PII is covered by the NRCS-1 SORN

10.10 Does the system use web measurement and customization technology?

- No, the system does not use web measurement and customization technology.

10.11 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?

- Not applicable, FPAC Box is a SaaS technology

10.12 Privacy Impact Analysis: 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.

- Privacy risks are nominal. FPAC Box does not control, link or provide access to third-party applications. Access is controlled by USDA's role-base authorization and eAuthentication process.

Agency Responsible Officials

KURT BENEDICT Digitally signed by KURT BENEDICT
Date: 2021.03.08 15:22:26 -06'00'

Kurt Benedict
FPAC Box Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS Digitally signed by LANITA THOMAS
Date: 2021.03.05 17:11:09 -05'00'

Lanita Thomas
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2021.03.03 13:12:51 -06'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture