Privacy Impact Assessment

FPAC DevSecOps Pipeline FPAC Moderate (Pipeline FPAC Mod)

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: January 13, 2022
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

FPAC DevSecOps Pipeline FPAC Moderate

January 2022

Contact Point

Doug Jones
Information System Owner
816-926-2758

Reviewing Official

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

Abstract

The FPAC DevSecOps Pipeline FPAC Moderate (Pipeline FPAC Mod) is a PaaS platform located in the FPAC AWS GSS environment. This system hosts several FPAC Moderate applications. The TeamMate+ (TeamMate+) and Digital Record Management System (DRMS) applications contain PII.

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

While moving systems & applications to the Cloud, FPAC is merging several systems into "Pipeline systems". One of these systems is FPAC DevSecOps Pipeline FPAC Moderate (Pipeline FPAC Mod). Pipeline FPAC Mod is a PaaS platform located in the FPAC AWS GSS environment. This system will host several FPAC Moderate applications. Currently, the TeamMate+ (TeamMate+) and Digital Record Management System (DRMS) applications are being migrated to FPAC Mod, and both contain PII. This PIA supports State laws, regulations, and USDA policies.

The Pipeline FPAC Mod is a combination of the following FBC systems with PII:

1. **TeamMate+ (TeamMate+)** - is an electronic audit management tool that supports audit functions performed by the FBC Performance, Accountability and Risk Internal Auditing Branch and the various other groups within the Agency that perform auditing functions. TeamMate+ provides real-time collaboration opportunities for the Internal Auditing Branch (IAB) and IAB's stakeholders Branches (FSA, NRCS and FBC). It includes the ability to manage national level compliance audits, ad-hoc reviews, risk assessment activities and tracking capabilities of external audits status and corrective actions. The primary users of this application include the Internal Auditing Branch and the External Audits and Investigations Branch.

2. **Digital Record Management System (DRMS**) - The Digital Record Management System (DRMS) is a cloud system that resides on FPAC_AWS_Shared_GSS (FPAC_AWS_GSS). DRMS replaces manual, paper-based business processes to a comprehensive digital record management system to manage end-to-end lifecycle of both permanent and temporary records. With NARA-compliance in mind, DRMS acts as the system of record for all the metadata about these records and supports indexing and search capabilities. Paper Documents are scanned using Kofax and ingested via DRMS bulk ingestion or scan-on-demand. Metadata checks are conducted before scanned documents go into the Alfresco database, the metadata for scanned documents are stored in Elasticsearch database for instant retrieval when needed.

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?

Application	No PII Collected	Name	Date or Place of Birth	Address or email address	PIN/SSN	Financial Data	Health Data	Biometric	Criminal History	Employment History	Misc. ID numbers	Photos or images	Handwriting or signature	Other	Notes
DRMS		X		X	X	X					X	X		X	See Note A
TeamMate+	X	X	X	X	X	X				X	X	X	X		See Note B
Note A	DRMS collects scanned paper records to include digitized forms and its related metadata. DRMS data may include a wide range of PII in the areas of financial, natural resources, and general information. Note: The information is stored in PDF files and is not collected via data entry fields. Potential PII found in the encrypted documents includes: Name, Legal Name, Address, Tax ID number (individual or business), SSN, Data Universal Numbering System (DUNS) number, Registration in Central Contractor Registration database, Legal description of farm location, Tract Number, Deeds, Farm Shareholder salaries, Location, Farm ownership detail, Bank routing numbers, Deposit Account numbers, Contract numbers, Vendor ID.														
Note B	The data could be in the form of Financial Management, Human Resources, Grants and Agreements, Purchase Cards, Real Property, Producer Applications, Producer Payments, Producer Contracts and Producer Records.														

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

Application	Sources of information in application
DRMS	DRMS collects scanned paper records to include digitized forms and its related metadata. This information may have been submitted to the system from field offices, FPAC digital content and metadata from Alfresco store at the Digital Infrastructure Services Center (DISC).
TeamMate+	Data will be in the form of audit "Provided by Customer" documents. The Internal Auditing Branch audits all programs and administrative areas of the USDA FPAC mission area. This data could be produced by any Division, Branch, State, County, or National Office of FPAC this includes FBC (FPAC Business Center),

	NRCS, FSA, or RMA. The data could also be produced by customers of FPAC, this can include private individuals, cooperatives, other local, state, and federal governments and it could include non-government organizations (the data could be in the form of Financial Management, Human Resources, Grants and Agreements, Purchase Cards, Real Property, Producer Applications, Producer Payments, Producer Contracts and Producer Records).

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

Applications	Why information being collected, used, disseminated or maintained.
DRMS	The information is being collected for the purpose of storage and retrieval for business needs. All staff are able to upload and search for documents, limited by their organizational role and rights. Specialized roles for records managers and legal staff allow for lifecycle management of records or unconstrained searching for audit, legal discover, litigation holds, or Freedom Of Information Act inquiries.
TeamMate+	The data is used in the FPAC financial audit process and serve as proof/documentation of findings. Audits are completed to identify program and administrative controls that are not adequate and allow for errors to be made. These errors can result in (Improper Payments, Improper Contracts, Improper Agreements, Ineligible Producers that were deemed eligible)

1.4 How is the information collected?

Applications	How information collected.
DRMS	The information is collected when scanned into the system and into the databases. Databases: MS SQL Database, Alfresco database, Elasticsearch database.
TeamMate+	The data can be either uploaded directly into TeamMate+ by the customer (most common) or it can be uploaded by auditors (in rare cases).

1.5 How will the information be checked for accuracy?

Validation against schema for each doc type and other reference tables containing information from NRT. Additionally, Client-side validation and human user review processes are used to validate data.

DRMS: No data verification occurs inside DRMS, however, the DRMS data consists of PDF documents originated by users, (so data is self-checked by the provider of the information).

TeamMate+: No data validation is provided for in TeamMate+. However, data uploaded by customers is self-checked. Data uploaded by auditors is subject to audit verification if relevant to the audit objectives.

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

- For FPAC-P, Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397, the Agricultural Act of 2014 (Pub. L. 113-79), the Agricultural Improvement Act of 2018 (Pub. L. 115-334), and the Coronavirus Aid, Relief, and Economic Security Act (CARES ACT) (Pub. L. 116-136)
- USDA RCPP Program (http://www.grants.gov/view-opportunity.html?oppId=291192)
- The Regional Conservation Partnership Program (RCPP) is authorized by Subtitle I of Title XII of the Food Security Act of 1985 (the 1985 Act), as amended by Section 2401 of the Agricultural Act of 2014 (the 2014 Act). The Secretary of Agriculture has delegated the authority to administer RCPP to the Chief of the Natural Resources Conservation Service (NRCS), who is Vice President of the Commodity Credit Corporation (CCC). NRCS is an agency of the Department of Agriculture (USDA).
- USDA CAET program
- USDA TSP Program: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/programs/technical/tsp/

These regulations pertain:

- 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.

- Privacy risk are moderate as privacy information is inputted only by partners and NRCS government employees that have access to the application. Under our current plan, users must be authenticated via USDA ICAMs e-AUTH system and authorized via USDA's role-based authorization
- The minimum amount of personally identifiable information is collected to satisfy the purpose of this system. The risks are mitigated using various control mechanisms, these include:

- All users must be uniquely identified and authenticated prior to accessing the application.
- Access to data is restricted.
- Information is encrypted at rest and in transit.
- Masking of PII.
- System audit logs are retained and reviewed weekly.

Section 2.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Applications	Uses of information.
DRMS	The information is securely stored for retrieval when needed for a business use by FPAC. All staff are able to upload and search for documents, limited by their organizational role and rights. Specialized roles for records managers and legal staff allow for lifecycle management of records or unconstrained searching for audit, legal discover, litigation holds, or Freedom Of Information Act inquiries.
TeamMate+	The data are used in the FPAC financial audit process and serve as proof/documentation of findings. Audits are completed to identify program and administrative controls that are not adequate and allow for errors to be made. These errors can result in improper payments, contracts and agreements as well as ineligible producers that were deemed eligible, etc.,

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

For DRMS only form data and JavaScript Object Notation (JSON) metadata will be produced. Adobe PDF plug-ins are used to view the documents. JASON metadata is the standard for describing data documents. A metadata file written in JSON is used to configure the fields and categories for document abstraction. Metadata JSON files may be used to control a variety of implementation specific configurations, such as understanding common fields of a specific type of cancer report or case file.

For TeamMate+, humans (auditors) are used to review the data for incorrect completion, incompleteness, conflicts with policy, etc. The final product of an audit is a report which can be hard copy, virtual, or recorded. The report provides the customer with the answers to the report objectives and specifically identifies findings with the five elements condition, criteria cause, effect, and recommendation. The

recommendation is the action needed to address the findings root cause and improve the lacking control.

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

N/A: No commercial or publicly available data is maintained in either DRMS or TeamMate+.

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.

- Access to the system and data are determined by business need and individual roles. Controls are in place to provide reasonable assurance that data integrity and confidentiality are maintained during processing. Controls in place to ensure the correct handling of information include the following:
  - End users are correctly identified and authenticated according USDA and FSA security policies for access managements, authentication and identification controls.
  - Audit logging is performed at the Department-level to ensure data integrity.

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?

This section only applies to applications that retain records; some applications will not retain records therefore these applications do not have a retention period.

Applications	Retention of information
DRMS TeamMate+	All information contained will be retained in compliance with NARA Guidelines, which vary on average in years from less than one year to more than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017.

	Per the NRCS-1 System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs."

The archiving and retention strategy for applications on Pipeline FPAC Mod will be retained in accordance with the NARA Retention Schedule. Information on most applications is retained indefinitely (permanent records).

See Record Retention Policy: https://usdagcc.sharepoint.com/sites/FBC-RecMS-Public/rmlibrary/Forms/AllItems.aspx

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

Yes, in accordance with NARA General Records Schedule Authority. Any deviations from the NARA Retention Schedule will be approved by NARA when the archiving and retention strategy is defined.

https://usdagcc.sharepoint.com/sites/FBC-RecMS-Public/rmlibrary/Forms/AllItems.aspx

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 retention period is based on a combination business need (i.e., how long do we need this information for our business process) and long-term usefulness. When records have reached their retention period, they are immediately retired or destroyed in accordance with the USDA Record Retention policies and procedures.

During this period, the stored information may be at risk for viewing by unauthorized parties, data loss or destruction and non-availability. Access to computerized files are protected by access control software, physical access controls and if warranted, password-protected.

According to Records Management DR3080-001 Disposition of Inactive Records:

Records and other documents that are no longer sufficiently active to warrant retention in office space shall be removed as rapidly as possible by: (a) transfer to a Federal Records Center, or (b) transfer to a records retention facility meeting the requirements of 36 CFR Chapter 12, Subchapter B Records Management, Subpart K, 1228.224 through 1228.244, or (c) if authorized, by disposal. (See Appendix B – Records Disposition Procedures.)

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?

Applications	Internal organization(s) in which information is shared, what information is shared and for what purpose?
DRMS	N/A (not shared)
TeamMate+	N/A Everything generated or held by the Internal Auditing Branch is for internal use only.

4.2 How is the information transmitted or disclosed?

Applications	Information transmittal / disclosure
DRMS TeamMate+	N/A

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.

Applications	Privacy risks associated with the sharing and how they were mitigated
DRMS TeamMate+	N/A

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?

Applications	External organization(s) in which information is shared, what information is shared and for what purpose?
DRMS TeamMate+	N/A (No application information is not shared outside of the USDA environment)

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.

Applications	External PII sharing compatibility and SORN coverage, or legal mechanisms by which system is allowed to share PII
DRMS TeamMate+	N/A Data is not shared with external organizations.

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

Applications	Externally shared information and security measures
DMS TeamMate+	N/A

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

Applications	External sharing privacy risks and mitigation
DRMS TeamMate+	N/A.

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.

Yes, in that FPAC Business Center (FBC) is the management organization in which Pipeline FPAC Mod resides, the legal authority to capture limited PII data for FPAC systems are established in the following Systems of Records Notices (SORNs):

- NRCS records are subject to: USDA/NRCS-1
- FSA records are subject to: USDA/FSA–2 - Farm Records File (Automated) and USDA/FSA-14 - Applicant/Borrower.
- RMA records are subject to:
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-1.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-2.txt ;
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-3.txt ;
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-4.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-5.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-6.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-7.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-8.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-9.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-10.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-11.txt

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

Yes, notice is provided to the individual prior to collection of information. The notice is provided to individual at the time of logging into the applications.

The FPAC Privacy Policy is published on the USDA website. In addition, when accessing an application that requires a sign in, an approved Level 2 eAuth login and password is required. If the individual has approval, the USDA OCIO eAuth banner provides the required notice upon accessing the application.

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

Applications	Individual's right to decline to provide PII information
DRMS TeamMate+	Yes, individuals may choose not to include privacy information in their correspondence, in accordance with USDA Privacy Policy, which states that submitting information is strictly voluntary. Please see: https://www.fsa.usda.gov/help/privacy-policy/index

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

Applications	Individual's right to consent to uses of PII and how exercised
DRMS TeamMate+	Yes, individuals may can choose that information not be used for specific purposes in accordance with USDA Privacy Policy and the individual's

	written consent. Please see: https://www.fsa.usda.gov/help/privacy-policy/index

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.

Notification is automatically provided in the system of records notices (Federal Register publications):

- NRCS: USDA/NRCS-1
- FSA: USDA/FSA–2 - Farm Records File (Automated) and USDA/FSA-14 - Applicant/Borrower.
- RMA:
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-1.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-2.txt ;
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-3.txt ;
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-4.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-5.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-6.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-7.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-8.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-9.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-10.txt
  https://www.ocio.usda.gov/sites/default/files/docs/2012/FCIC-11.txt

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?

Individuals do not have access to DRMS and TeamMate+. Authorized FPAC staff has access to the documents maintained in the applications and they are able to update incorrect information. As published in FPAC's SORN's, "An individual may obtain information about a record in the system which pertains to such individual by submitting a written request to the above listed System Manager. The envelope and letter should be marked ``Privacy Act Request.'' A request for information should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

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

Authorized FPAC staff has access to the documents maintained in DRMS & TeamMate and they are able to update incorrect information. Individuals who are aware of potential incorrect information can contact FPAC staff via the Help Desk or CCG to request resolution. Instructions for procedures to request a correction are also posted on USDA's OCIO website: https://www.ocio.usda.gov/policy-directives-records-forms/guidelines-quality-information/correction-information

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

Individuals are notified by FPAC staff regarding procedures to update incorrect information. Formal redress is provided on the USDA/OCIO website: Correction of Information | Office of the Chief Information Officer (usda.gov)

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

- N/A. The SORN USDA/NRCS-1 is published on the USDA.gov website. The USDA SORNs are published on the USDA OCIO System of Records website. https://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records

- As published in SORN USDA/NRCS-1: "Any individual may obtain information as to the procedures for contesting a record in the system which pertains to him/her by submitting a written request to the district conservationist or his/her designated representative or to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013."

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

Residual privacy risks associated with the redress process for individuals are mitigated since individuals can use the relevant procedures discussed above to update their original public records.

For DRMS and TeamMate+, the risk associated with redress is considered low, as the public does not have access to the system or the data. While the public cannot access the system to update or change their personal information, they may update their information

and submit the information to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

As published in SORN USDA/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

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?

DRMS access is determined via a Level 2 eAuth ID and password on a valid need-to-know basis, determined by requirements to perform applicable official duties. DRMS has documented Access Control (AC) Procedures, in compliance with FISMA and USDA directives. 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 (SP) 800-53, Revision 4.

TeamMate+ End Users, use the PIV or eAuth Credentials application through eAuth application to access TeamMate Plus. Access granted to end users, is approved by IAL2 and are given privileges based on a least privileged model. Administrators, access to the TeamMate Plus application is restricted to 5 number of people. Administrator access can only be achieved by remote access and requires PIV or eAuth credentials authentication. Local access is restricted to remote access/console login for administrative and configuration purposes possible (if configured that way) made due to this application server being in the AWS datacenter.

8.2 Will Department contractors have access to the system?

- Yes. Department contractors with a need-to-know will have access to Pipeline FPAC Mod as part of their regular assigned duties.

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

Annual organizational Information Security Awareness Training is mandatory for all FPAC personnel. FPAC requires that every employee and contractor receive 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.
To remind users of their responsibilities (which they acknowledged during their Annual Information Security Awareness Training), the application reiterates that documents passed to Document Management System (DMS) may contain sensitive information, and this information must not be disclosed to anyone unless the recipient has a direct need-to-know in the performance of their official duties.

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

Applications on this system were originally on systems with valid ATOs; these applications were moved to Pipeline FPAC Mod, which will receive an ATO.

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 these applications per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 4. Additionally, the system provides technical safeguards to prevent misuse of data including:
  - Confidentiality: Encryption is implemented to secure data at rest and in transit for these applications (e.g., by FIPS 140-2 compliant HTTPS and end-user hard disk encryption).
  - Integrity: Masking of applicable information is performed for these applications (e.g., passwords are masked by eAuth).
  - Authentication: Access to the system and session timeout is implemented for these applications (e.g., by eAuth and via multi-factor authentication for remote access).

  Additionally, these and other safeguards are in place:

  - Access Control: The system 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.
  - Audit: Logging is implemented for these applications (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?

- Privacy concern involving collection information is mitigated by the use of encryption, controlled access, and system audits.
- Privacy risks are mitigated as PII information is minimal and is only accessed and handled by FPAC-authorized roles and e-authenticated personnel.
- Data extracts containing PII are not regularly obtained from the system, therefore, privacy risk from this area is limited and addressed through IT Data Extract processes controls.
- For DRMS and TeamMate+, the main risk associated with privacy is the exposure to unauthorized access to privacy information. This risk is considered moderate. Mitigating controls are in place to ensure privacy risks are minimal. Mitigated controls are mapped back to SSP in CSAM.
- Quarterly access reviews are done to ensure controls are mitigated.

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?

- All applications on Pipeline FPAC Mod are applications. Pipeline FPAC Mod resides on the USDA GovCloud Platform.

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

No applications on this system employ technology which raise privacy concerns.

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, the System Owner and ISSPM for Pipeline FPAC Mod have reviewed these memorandums.

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

N/A, 3rd party websites are not used.

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

N/A, 3rd party websites are not used.

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

N/A, 3rd party websites are not used.

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?

N/A, 3rd party websites are not used.

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

N/A, 3rd party websites are not used.

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

N/A, 3rd party websites are not used.

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?

N/A, 3rd party websites are not used.

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)?

N/A, 3rd party websites are not used.

10.10 Does the system use web measurement and customization technology?

No, Pipeline FPAC Mod applications do 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?

N/A, Pipeline FPAC Mod applications do not use web measurement and customization 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.

N/A - privacy risks of data becoming available via 3rd party websites are minimal in that these applications (DRMS, TeamMate+), nor does Pipeline FPAC Mod use web measurement or customization technology.

Agency Responsible Officials

DOUGLAS JONES Digitally signed by DOUGLAS JONES
Date: 2022.01.18 13:02:50 -06'00'

Doug Jones
Information System Owner
United States Department of Agriculture

Agency Approval Signature

BRIAN DAVIES Digitally signed by BRIAN DAVIES
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=BRIAN DAVIES, 0.9.2342.19200300.100.1.1=12001000000604
Date: 2022.01.19 11:19:59 -05'00'

Brian Davies
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2022.01.19 14:35:31 -06'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture