Privacy Impact Assessment
Digital Records Management System (DRMS)

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: January 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

Digital Records Management System (DRMS)

January 19, 2021

Contact Point

Julia Oswald
IT Project Manager
julia.oswald@usda.gov
816-926-6273

Reviewing Official

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

Abstract

The Digital Record Management System (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. Initially, bulk scanning of paper records and metadata extraction will be staged and retrieved using a bulk submission to metadata stores.

This PIA is being conducted to comply with Federal Information Security Management Act (FISMA) of 2002 and the E-Government Act of 2002 (Public Law. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) Federal Law.

Overview

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 document management business processes with a comprehensive digital record management system able to support the end-to-end lifecycle of both permanent and temporary records. With NARA-compliance in mind, DRMS acts as the system of record for both electronic records and the metadata necessary to describe those records. DRMS offers indexing and search capabilities that allow manual or automated uploading of electronic records and subsequent retrieval of relevant records for operational, legal and records management purposes. No financial transactions occur via DRMS.

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?

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

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

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).

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

The information is being collected for the purpose of storage and retrieval for business needs.

1.4 How is the information collected?

The information is collected when scanned into the system and into the databases

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. No data verification occurs inside DRMS.

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

The following 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.

Possible privacy risks include data leakage and insecure data transfer. Encryption has been implemented data at rest and in transit.

These Privacy risks are mitigated because access to the information is limited to appropriate FPAC personnel and partners through the use of the eAuth application, which provides user authentication for FPAC. Other access requirements include the need for users to be on the USDA network backbone, using a USDA computer, and via FPAC's role-based authorization (RBAC).

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.

The information is securely stored for retrieval when needed for a business use by FPAC.

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

Only form data and JSON metadata will be produced. Adobe PDF plug-ins are used to view the documents

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 DRMS

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 (SP) 800-53, Revision 4.
If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes

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 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."

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

Per NARA Code of Federal Regulations - 36 CFR 1220, Subchapter B – Records Management and USDA OCIO Department Regulation 3080-001 accessible at:
http://www.ocio.usda.gov/document/departmental-regulation-3080-001
NARA Approval: NARA approval is required for all official records schedules. SF-115 shall be submitted to NARA for approval. External approval has already been granted for records covered by the General Records Schedules (GRS). No external approval is required for the disposition of non-record materials. An informational copy of the SF-115, in both hard copy and electronic format, shall be provided to the Departmental Records Officer at the same time that the original is sent to NARA.
Electronic Records: Electronic records should be scheduled in the context of entire information systems, along with appropriate documentation and related indexes, and provide the necessary elements:

• All input records or source documents.
• All information recorded on electronic media.
• All output records.
• The documentation associated with the system.
• Any related indexes.

As with audiovisual and microform records, permanent electronic records should not be proposed for long-term storage at Federal records centers but should be transferred directly to the National Archives.

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

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?

N/A. Information is not shared.

4.2 How is the information transmitted or disclosed?

Information is encrypted in transit using HTTPS.

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.

Only USDA employees are allowed access to the data stored in the system. Additionally, privacy risks are mitigated by minimizing the data shared outside DRMS.

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?

N/A - DRMS data is not be shared with external organizations

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.

N/A - DRMS data is not be shared with external organizations

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

N/A - DRMS data is not be shared with external organizations

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

N/A - DRMS data is not be shared with external organizations

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. This application is subject to the NRCS-1 SORN accessible at:
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?

Yes. 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.
Refer to the USDA FPAC Privacy Policy accessible at:
https://www.nrcs.usda.gov/wps/portal/nrcs/detailfull/national/about/?cid=nrcsdev11_000885

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

Yes; individuals can choose to not include any privacy information in their correspondence.

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

Yes; individuals can choose to not include any privacy information in their correspondence, or to not provide correspondence. Once received, however, USDA is required to maintain the correspondence.

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.

Notice is provided via the USDA SORNs

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. Authorized FPAC staff has access to the documents maintained in DRMS and they are able to update incorrect information.

As published in NRCS-1 SORN: "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.)."

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

Authorized FPAC staff has access to the documents maintained in DRMS 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.
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.)."

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. The SORN USDA/NRCS-1 is published on the USDA.gov website.

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

N/A. Refer to Section 7.3

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

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.)." 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.

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 DRMS 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. Please refer to Section 2.4 for further information.

8.2 Will Department contractors have access to the system?

Yes. Department contractors with a need-to-know will have access to DRMS as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements.

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 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 Security Awareness Training), the application reiterates that documents passed to DRMS 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?

No. DRMS anticipates the initial ATO around March 1, 2021.

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

FPAC complies with the FISMA of 2014. Assessment and Accreditation (A&A), as well as annual key control self-assessments and continuous monitoring procedures are implemented for PDS per the requirements given in NIST SP 800-53 Revision 4. The system also provides technical safeguards to prevent misuse of data including the following:

- Confidentiality: Encryption is implemented to secure data at rest and in transit for PDS [e.g., by Federal Information Processing Standards (FIPS) 140-2 compliant HTTPS and end-user hard disk encryption]. The documents that are passed to, and maintained in, DRMS are encrypted in transit.
- Integrity: Masking of applicable information is performed for PDS (e.g., passwords are masked by eAuth).
- Access Control: PDS implements least privileges and need-to-know to control access to PII [e.g., by Role-Based Access Control (RBAC)].
- Authentication: Access to the system and session timeout is implemented for PDS (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: Logging is implemented for PDS [there is a logging infrastructure including Application Audit Log Solution (AALS)]. PDS logs events from various devices within its

accreditation boundary to include web servers and database servers. FPAC logs data transactions from devices adjacent to the PDS accreditation boundary to include the legacy databases and the CA Application Programming Interface (API) Gateway. Logged events will be stored in the FPAC Security Information and Event Management (SIEM) server.

- Attack Mitigation: The system implements security mechanisms such as input validation.

Note: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

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?

Any 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 Sections 4 and 5 respectively. Remediation of privacy risks associated with notice and redress are addressed in Sections 6 and 7 respectively.

Mitigation occurs through policies that address Separation of Duties (SOD) which ensures that system operators and system administrators have limited, if any, access to PII. In addition, NIST 800-53 Audit and Accountability (AU) audit controls are used to prevent data misuses.

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?

The application is Cloud based, developed by a Contractor for use by the USDA. This system has both front end applications (DRMS) as well as back-end computing /processing applications (inherited from the host GSS).

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

No. DRMS utilizes USDA-approved technologies and these technology choices do not 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.

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

The KOFAX application enables the capture of paper documents to transferred to electronic.

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

N/A - No PII is shared with external organizations.

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 - No PII is shared with external organizations.

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 - No PII is shared with external organizations.

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

N/A - No PII is shared with external organizations.

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 - No PII is shared with external organizations.

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 - No PII is shared with external organizations.

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)?

Not Applicable. DRMS does not use 3rd party websites or applications.

10.10 Does the system use web measurement and customization technology?

Not Applicable. DRMS does not use web measurement or 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. DRMS does not use web measurement or 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.

Privacy risks of DRMS data becoming available via 3rd party websites are nominal. In addition, DRMS does not use web measurement or customization technology

Agency Responsible Officials

KURT BENEDICT

Digitally signed by KURT BENEDICT
Date: 2021.02.11 10:00:55 -06'00'

Kurt Benedict
DRMS 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: 2021.02.09 18:30:05 -05'00'

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

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2021.02.11 06:01:13 -06'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture