Privacy Impact Assessment

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment

Privacy Impact Assessment for the USDA IT System/Project:

AgWrite Content Management System (CMS)

Office of the Executive Secretariat

Date PIA submitted for review:

February 20, 2024

Mission Area System/Program Contacts:

	Name	**E-mail**	**Phone Number**
Mission Area Privacy Officer	*Michele Washington*	*Michele.Washington@usda.gov*	*202-577-8021*
Information System Security Manager	*Tracy Haskins*	*Tracy.Haskins@usda.gov*	*202-264-0135*
System/Program Managers	*Marcia Moore*	*Marcia.Moore@usda.gov*	*202-713-8054*

Abstract

The U.S. Department of Agriculture (USDA) receives thousands of pieces of correspondence and documents and is implementing a new platform called AgWrite, a modernized content management system managed by the USDA Office of Executive Secretariat (OES). The new system will implement advanced technology to transform how correspondence is processed in OES, supporting standardized processes and role-based access. The Privacy Impact Assessment (PIA) is being conducted to ensure that personally identifiable information (PII) voluntarily provided by public individuals and organizations is properly safeguarded and controlled while being handled and managed in the system.

Overview

AgWrite is a content management (CMS) system owned and managed by the Office of the Executive Secretariat (OES). AgWrite is being leveraged to provide standardized processes and role-based controls to support the receipt and processing of correspondence and other artifacts that require ingestion, review, and approval by business units across USDA. AgWrite supports the OES mission by providing a centralized system where users can access and interact with information to promote expedient facilitation of correspondence receipt and processing. The system will include information regarding individuals, primarily information such as the name, address, phone number, and email address incidental to their correspondence addressed to the Secretary of Agriculture and various other officers and employees of USDA. In a few cases, it may also include other information about the individual voluntarily provided by that individual in the correspondence. A typical transaction in the system is a user accessing a package record, reviewing the content and metadata, documenting changes to the metadata or producing research or a response to received correspondence, and tracking the movement of the packages between different users and user groups.

Section 1.0 Authorities and Other Requirements

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

4 U.S.C. 3101, et seq.; 44 U.S.C. 3504 note; 44 U.S.C. 3501, et seq.; 44 U.S.C. 3541, et seq. provide AgWrite the legal authority to collect information. Additionally, the collection of documents is governed by 5 U.S.C. § 301 (general agency powers for recordkeeping) and the Privacy Act of 1974, as amended (5 U.S.C. § 552a). Pursuant to 5 U.S.C. § 301, USDA is authorized to implement regulations that manage USDA's day-to-day operations. These operations include regulating employees, managing agency business, and controlling agency papers and property.

1.2 Has Authorization and Accreditation (A&A) been completed for the system?

The system is currently in development. The A&A process has begun and is in progress with an assigned Information System Security Officer (ISSO).

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

Correspondence and Document~~AgWrite Content~~ Management System, OES-2

1.4. Is the collection of information covered by the Paperwork Reduction Act?

No. Information collected by OES-2 is not considered to be "Information" under the PRA.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers			
☐	Social Security number	☐	Truncated or Partial Social Security number
☐	Driver's License Number	☐	License Plate Number
☐	Registration Number	☐	File/Case ID Number
☐	Student ID Number	☐	Federal Student Aid Number
☐	Passport number	☐	Alien Registration Number
☐	DOD ID Number	☐	DOD Benefits Number
☐	Employee Identification Number	☐	Professional License Number
☐	Taxpayer Identification Number	☐	Business Taxpayer Identification Number (sole proprietor)
☐	Credit/Debit Card Number	☐	Business Credit Card Number (sole proprietor)
☐	Vehicle Identification Number	☐	Business Vehicle Identification Number (sole proprietor)
☐	Personal Bank Account Number	☐	Business Bank Account Number (sole proprietor)
☐	Personal Device Identifiers or Serial Numbers	☐	Business device identifiers or serial numbers (sole proprietor)
☒	Personal Mobile Number	☒	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number		

Biographical Information					
☒	Name (including nicknames)	☐	Gender	☒	Business Mailing Address (sole proprietor)
☒	Date of Birth (MM/DD/YY)	☐	Ethnicity	☒	Business Phone or Fax Number (sole proprietor)
☐	Country of Birth	☐	City or County of Birth	☒	Group/Organization Membership
☐	Citizenship	☐	Immigration Status	☐	Religion/Religious Preference
☒	Home Address	☒	Zip Code	☒	Home Phone or Fax Number
☐	Spouse Information	☐	Sexual Orientation	☐	Children Information
☐	Marital Status	☐	Military Service Information	☐	Mother's Maiden Name
☐	Race	☐	Nationality	☐	Global Positioning System (GPS)/Location Data
☒	Personal e-mail address	☒	Business e-mail address	☐	Personal Financial Information (including loan information)
☐	Employment Information	☐	Alias (username/screenname)	☐	Business Financial Information (including loan information)
☐	Education Information	☐	Resume or curriculum vitae	☐	Professional/personal references
Biometrics/Distinguishing Features/Characteristics					
☐	Fingerprints	☐	Palm prints	☐	Vascular scans
☐	Retina/Iris Scans	☐	Dental Profile	☐	Scars, marks, tattoos
☐	Hair Color	☐	Eye Color	☐	Height
☐	Video recording	☐	Photos	☐	Voice/ Audio Recording
☐	DNA Sample or Profile	☐	Signatures	☐	Weight
Medical/Emergency Information					
☐	Medical/Health Information	☐	Mental Health Information	☐	Disability Information
☐	Workers' Compensation Information	☐	Patient ID Number	☐	Emergency Contact Information
Device Information					
☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data
Specific Information/File Types					
☐	Personnel Files	☐	Law Enforcement Information	☐	Credit History Information
☐	Health Information	☐	Academic/Professional Background Information	☐	Civil/Criminal History Information/Police Record
☐	Case files	☐	Security Clearance/Background Check	☐	Taxpayer Information/Tax Return Information

2.2. What are the sources of the information in the system/program?

Information in this system of records is primarily provided by the individual corresponding with USDA or Agency officials, such as managers and supervisors, responding to individuals, organizations, or Members of Congress. Sources of information include:

- The White House
- The Vice President
- Federal Agencies
- Congress
- State and Local Governments
- Foreign Officials
- Corporations
- Non-Profit Organizations
- The General Public

2.2.1. How is the information collected?

The information is collected through the receipt of physical letters and electronic mail. Received correspondence is scanned through an optical character recognition software service that saves some contact elements of an individual into a database where it will assist USDA in responding to their correspondence.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

Yes, the system expects to use business, organizational and governmental-level contact data that is traditionally available to the public. AgWrite will store data as it relates to individual and group-level contacts so that correspondence responses can be properly directed to the correct locations.

2.4. How will the information be checked for accuracy? How often will it be checked?

Information will be reviewed by multiple parties to ensure that the data provided by a correspondent matches the information entered and stored in the system. USDA employees will perform a “front end” review of records created to ensure that incoming documents and associated metadata are captured and categorized accurately. Furthermore, by nature of the review and approval process required to process Secretarial and other controlled correspondence, numerous checks and balances are in place to ensure that information is accurate, including a final quality assurance review performed by the record owner.

2.5. Does the system/program use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

Not applicable

2.5.1.1. What PII will be made available to the agency though the use of third-party websites?

None.

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

~~Follow the format below:~~

Privacy Risk: There is a risk that we may over collect PII from the public as part of the correspondence.

Mitigation: To mitigate this, ~~all system users must be USDA employees or contractors who have taken security and privacy training and granted access to the through role-based access control. Users only have access to information on a need-to-know basis, in order to perform their intended job function.~~ t~~T~~o the extent possible to process or archive a record, PII is redacted by the initial recipients of the correspondence. We also mitigate the privacy risk by ensuring that all received correspondence goes through an initial vetting process where sensitive information such as date of birth will be redacted from received items and will only be available to privileged users, if necessary.

Commented [DL1]: This is a 'use' risk and should be used below.

The risk for this section should say that there is a risk that we may over collect PII from the public as part of the correspondence and how we will mitigate that. Please update.

Section 3.0 Uses of the Information

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

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

Information is being collected and used to process correspondence for review and, if necessary, produce reports, and/or process and manage responses to answer questions or requests sent to USDA.

Physical and e-mail addresses will be particularly maintained for correspondence purposes. Phone numbers may be used to contact individuals for more information. Other information in the system will be used to document proposed policies and program activities for approval by USDA officials.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

Yes, the system will use enhance searching capabilities driven by Natural Language Processing (NLP) and Machine Learning (ML) to return results based on historical content and responses from similar inquiries. The use of NLP and ML technologies will also provide analysis on the historical classification of correspondence and documents.

To analyze data, Appian tasks, dashboards, and reports will be used. Search data produced could pertain to correspondence as they progress through workflows within the system (e.g., stage/status agency, priority or categorization, time in a particular status, time to progress from initiated to completed, congressional inquiries, etc.).

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

~~Follow the format below:~~

Privacy Risk: There is a risk that personal information provided by a correspondent could be inappropriately accessed by AgWrite system users. ~~to~~ The scope of the information collected in the CMS is limited to the amount of data necessary to act upon the request, correspondence, or other possible action item received by USDA. Although each correspondence is very likely to include the name of one or more correspondents, the signature on correspondence and other PII is voluntarily provided by the correspondents or is transmitted by the Executive Office of the President or their Congressional representative on their behalf.

Mitigation: To mitigate this, all system users must be USDA employees or contractors who have taken security and privacy training and granted access to the through role based access control. Users only have access to information on a need-to-know basis, in order to perform their intended job function. To the extent possible to process or archive a record, PII is redacted by the initial recipients of the correspondence. We also mitigate the privacy risk by ensuring that all received correspondence goes through an initial vetting process where sensitive information such as date of birth will be redacted from received items and will only be available to privileged users, if necessary

Section 4.0 Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

As information is voluntarily provided to the Department from unknown sources, there is no ability to provide notice to individuals prior to receipt of the information. However, this PIA and the applicable SORN serve ~~serves~~ as notice. ~~and that the applicable SORN also acts as notice.~~ =

4.2. What options are available for individuals to consent, decline, or opt out of the project?

Information, contained within Agwrite, is voluntarily provided to the Department from unknown sources, therefore, it is inherent that they are providing their consent.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

~~Follow the format below:~~

Privacy Risk: There is a risk that individuals corresponding with USDA will not be given proper notice prior to the collection of their information. ~~No notice given for the initial collection as the information is~~

Commented [DL2]: This is not a risk, this is a mitigation.

Commented [PB3R2]: Swapped risk and mitigation

Commented [DL4]: See updated risk.

~~voluntarily submitted without request. The information will be used only for the purpose stated in the AgWrite Content Management System, OES-2 SORN~~

Mitigation: This risk is partially mitigated. Although ~~N~~no notice is given for the initial collection as the information is voluntarily submitted without request, ~~.~~ ~~t~~The information will be used only for the purpose stated in this PIA and the~~e~~ ~~AgWrite Content~~ Correspondence and Document Management System, OES-2 SORN. ~~Sufficient notice will be provided through a SORN published in the Federal Register (FR). In the FR, the public will be allowed 30 days to provide comments and for the agency consideration.~~

Commented [DL5]: This should be the risk not the mitigation.

Commented [PB6R5]: Swapped risk and mitigation

Section 5.0 Data Retention

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

5.1. What information is retained and for how long?

The retention of data in the system is in accordance with applicable USDA records disposition schedules as approved by the National Archives and Records Administration (NARA). Records are maintained for varying periods, and temporary records are disposed of by shredding when the retention period is complete. Electronic records are sent to NARA, per the disposition document, after a period of five years. Records are maintained as an electronic copy in the system as needed for reference.

Commented [DL7]: Doesn't the record schedule have a disposition for these documents as well?

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

The records schedule N1-016-08-3 for Secretarial correspondence has been approved by the OCIO and the National Archives and Records Administration (NARA).

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.

Follow the format below:

Privacy Risk There is a risk that ~~we~~ USDA may retain correspondence data for too long ~~.e~~.

Mitigation: ~~Risk will be mitigated in the future by exploring publicly available data sets to ensure that important contact information is synchronized with known sources that are maintained and managed. This feature is pending review and implementation in future system iterations.~~This risk is mitigated because the retention of data in the system is in accordance with applicable USDA records disposition schedules as approved by the National Archives and Records Administration (NARA). Records are maintained for varying periods, and temporary records are disposed of by shredding when the retention

period is complete. Electronic records are sent to NARA, per the disposition document, after a period of five years.

Section 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Correspondence and contact information will be shared with a limited and approved user set that extends to all business units within USDA so that the appropriate offices will be able to respond to correspondence that has been sent to the Department.

The information will be transmitted using services established in the system security boundary, including the Appian Low-Code Platform, the USDA Microsoft O365 instance, and the future USDA AgRecords system, and potentially the Enterprise Data Analytics Platform & Toolset (EDAPT) platform. All systems within the system security boundary are only accessible from within the USDA network or through an approved USDA Virtual Private Network (VPN) connection. Users involved in the response draft/review/approval process may print documents and then scan and upload updated documents into the system, particularly those with wet ink signatures.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: There is a risk that approved users will share information received by the system with others that may or may not have a business need. This includes the ability to look up contact information to send correspondence responses and print hard copies of correspondence and contact information to facilitate the sending of said responses.

Mitigation: Risk is mitigated by managing users through access control policies, auditing users accessing the system, logging actions taken on the system, and requiring all access to the system to be done within the USDA network.

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

No sharing of information with external organizations is expected beyond sending correspondence responses to individuals and organizations that have requested a response.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Follow the format below:

Risk is N/A because there is no external sharing.

Section 7.0 Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

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

Individuals who want to: know whether this system of records contains information about them, access their records, or contest the contents of a record, should make a written request to the Director, Office of the Executive Secretariat, U.S. Department of Agriculture, 1400 Independence Avenue SW., Washington, DC 20250. Individuals must furnish the following information for their records to be located and identified:

A. Full name or other identifying information necessary or helpful in locating the record;
B. Why he or she believes the system may contain their personal information;
C. A statement indicating the type of request being made (i.e., access, correction, or amendment) and whether a personal inspection of the records or a copy of them by mail is desired;
D. Signature.

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

The information received in the original correspondence is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise. If inaccurate entries are discovered during the resolution of the correspondence record, the organization tasked with resolving the inaccuracy will contact the originating office. If the department has incorrect information on a correspondent or their respective records, then that data can be updated as needed in the system by the system manager or delegate. An audit trail is maintained on any and all changes.

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

Individuals will be notified of the procedures for correcting their information within the system by the Office of Executive Secretariat (OES) staff, who will notify the individual if additional information is required to process their correspondence. Contact information for the Office of the Executive Secretariat can be found at the following location: Contact USDA. The Agency Contact number is listed as follows: 202-720-7100. Individuals can contact OES and request that the system manager correct any inaccurate information in the system. Additionally, SORN record correcting procedures can be found within USDA SORN OES-2.

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

Not Applicable because redress is provided.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

~~Follow the format below:~~

Privacy Risk: There is a risk that USDA may collect incorrect information from submitted correspondence.

Mitigation:
Formal redress procedures are available and outlined in the ~~AgWrite Content~~Correspondence and Document Management System, OES-2 SORN. Individuals requesting correction or amendment of their records should follow the Notification Procedures and the Record Access Procedures and also identify the record or information to be changed, giving specific reasons for the change.

Individuals who want to know whether this system of records contains information about them, who want to access their records, or who want to contest the contents of a record, should make a written request to the Director, Office of the Executive Secretariat, U.S. Department of Agriculture, 1400 Independence Avenue SW., Washington, DC 20250. Individuals must furnish the following information for their records to be located and identified:
A. Full name or other identifying information necessary or helpful in locating the record;
B. Why you believe the system may contain your personal information;
C. A statement indicating the type of request being made (i.e., access, correction, or amendment) and whether a personal inspection of the records or a copy of them by mail is desired;
D. Signature.

Individuals wishing to request access to their records should follow the Notification Procedures. Individuals requesting access are also required to provide adequate identification, such as a driver's license, employee identification card, social security card, or other identifying document. Additional identification procedures may be required in some instances.

Formatted: Font: 11 pt
Formatted: Font: 11 pt
Formatted: Indent: Left: 0.01"

Section 8 Auditing and Accountability

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

8.1. How is the information in the system/project/program secured?

AgWrite provides auditing at the application, database, and network/operating system levels. The application is controlled by security attributes which only allow authorized users to access the system. The hosting environment also provides technical safeguards, such as encryption, to prevent misuse of data. Controls are in place to protect the data and prevent unauthorized access. Access controls are based on the principle of least privilege, which refers to granting the minimum required system resources to a user to enables them to perform their duties.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

Only users who have enabled USDA Active Directory credentials and have access to the USDA network will be able to access the system. This system uses role-based access control to assign privileges to system users. Access to the data will be determined through specified role-based permissions as authorized by the system owner. This role-based access control to AgWrite is based on the principle of

least privilege. The principle of least privilege states that a user may only have the minimum privileges on an information system to perform their assigned tasks. Role-based access controls, as implemented for AgWrite, allocate resources and associated permissions to specific users or groups of users. Access control procedures to determine which users may access the system. These procedures are documented in the System Security Plan and communicated to AgWrite application administrators. Only users responsible for processing Secretarial correspondence and other controlled correspondence will be granted access to the system. USDA staff with the appropriate permissions will authorize users to access the system. User requests will be confirmed and passed to the Agency User Administrator to receive a user account and be added to the appropriate Active Directory group. Once completed, The AgWrite User Administrators will assign the respective permissions commensurate with the user's role in the system.

8.3. How does the program review and approve information-sharing requirements?

N/A because information is only shared within USDA and not external to the Department.

8.4. Describe what privacy training is provided to users, either generally or specifically relevant to the program or system/project.

USDA Information Security Awareness Training & Acknowledgment of Rules of Behavior are required by all federal employees and contractors. Privacy and PII training is included in the Security Awareness and Rules of Behavior training required for all federal employees and contractors annually. An exam is provided following the training and the user must receive 70% or better to maintain or receive access to the information system.

Approval Signatures:

_____
Marcia Moore, Director of Office of the Executive Secretariat (OES)
System Owner
United States Department of Agriculture

_____
Michele Washington, Privacy Officer
OCIO
United States Department of Agriculture

_____
<CISO/ACISO>
<Agency>
United States Department of Agriculture

_____
Chief Privacy Officer
United States Department of Agriculture