Privacy Impact Assessment

Correspondence Management System (OES/CMS)

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: August 2018
- Prepared for: United States Department of Agriculture (USDA) Office of the Executive Secretary (OES)

Abstract

The U.S. Department of Agriculture (USDA) receives thousands of pieces of correspondence and documents requiring secretarial signature each month (i.e. congressional inquiries; requests for assistance; ideas for solving the challenges facing the agriculture community; internal departmental regulations and policy memorandums, and much more) from a diverse range of constituents across the Nation and internationally.

The system is called ABE and it is owned and managed by the USDA Office of the Executive Secretariat (OES). It is also labeled as the OES Correspondence Management System (CMS) in some documents and tracking systems. The system is a customer relationship management (CRM) system that 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. The privacy impact assessment (PIA) is being conducted to ensure that personally identifiable information (PII) voluntarily provided by public individuals and organizations is properly understood and controlled while being handled and managed in the system.

A Privacy Impact Assessment (PIA) is being conducted because information in the Correspondence and Document Management System (CDMS) may be considered personally identifiable information (PII).

Overview

The ABE system is owned and managed by the Office of the Executive Secretariat (OES). It is also labeled as the OES Correspondence Management System (CMS) in some documents and tracking systems. The system is a customer relationship management (CRM) system that 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. It supports the OES mission by providing a centralized system where necessary 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, and other contact information 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. The system is expected to leverage existing Microsoft software as a service (SaaS), including Azure for Government virtual machines (VMs), Dynamics 365, and Office 365 Multi-Tenant (O365-MT). It will be sharing information between those existing platforms. All of this information sharing will be governed by a system boundary being established for this system. Legal authority to operate the system is provided by 44 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.

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?

The system will collect distinct contact information about individuals sending correspondence to USDA including Name, Address, E-mail Address, Phone Number, and Organization-specific information. Additionally, people will send letters and other forms of correspondence where it is expected that they will provide personal information within the context of the correspondence. Expected items include account numbers, Social Security Numbers (SSNs), birth dates, and other forms of contact information not collected in the database or associated with a contact record. The system plans to heavily mitigate access to this unneeded personal information to ensure privacy protections.

The following information will be collected as data fields in the Microsoft Dynamics CRM for an individual contact:

- Full Name (including titles if provided)
- Addresses
- Phone Numbers
- E-mail Addresses

The following information may be provided to OES in letter form; however, it will not be collected as a data field in the Microsoft Dynamics CRM as an individual contact:

- Date of Birth
- SSN
- Account Numbers and other miscellaneous identification numbers

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

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. Non-USDA sources of information include: The White House, The Vice President, Federal Agencies, Congress, State and Local Governments, Foreign Officials, Corporations, Non-Profit Organizations, and The General Public.

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

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

1.4 How is the information collected?

The information is collected through receipt of physical letters and electronic mail. Received correspondence will be scanned through an optical character recognition software service that will save some contact elements of an individual into a database where it will assist USDA in responding to their correspondence. Non-PII metadata defining and categorizing the received correspondence will be entered and managed by OES and agency staff, and responses and research to the received correspondence will be produced and stored in a record as well.

1.5 How will the information be checked for accuracy?

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 folders created to ensure that incoming documents and associated metadata is 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 folder owner.

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

The collection of documents within ABE 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.

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

The scope of the information collected in CDMS 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 of the individual and other personally identifiable information is voluntarily provided by the correspondents.

The privacy risk is that information about an individual could be used to impersonate them. To mitigate this, all users of the system must be USDA users, have taken security and privacy

training, and be granted access to the system through a necessary, least permissible role or set of rules based on their job needs.

We also mitigate the privacy risk by ensuring that all received correspondence goes through an initial vetting process where sensitive information like SSN and Date of Birth will be redacted from received items and only be available to be accessed by privileged users if necessary. Furthermore, access to the computer system containing the records in this system is limited to those individuals who have been granted system access rights, and those who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

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.

Personal information will be used so that system users will know who and how to respond to correspondence. Particularly, physical and e-mail addresses will be maintained and used to send responses. Phone numbers may be used to contact an individual for more information.

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

Ephesoft Transact will provide optical character recognition (OCR) to evaluate all received materials so the text in them can be machine-readable. AvePoint Compliance Guardian will be used to redact sensitive personal information so that its exposure can be limited and controlled. Microsoft Dynamics will be used to organize and store the data so that users can access contact information and respond to correspondence as necessary to complete business transactions with groups and individuals corresponding with USDA. SharePoint Online will be used to store and manage received and produced artifacts that may contain contact information.

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

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

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.

PII communicated to the Department that is not necessary to accomplish the business task of responding to correspondence is expected to be redacted and/or not collected into defined data fields when entering the system accessible by most of the system users.

The concept of least permission will be established on user roles to ensure that users of the system only have access to the information necessary to do their job.

All users accessing the system will have taken USDA security and privacy training, will be required to authenticate to the USDA network, and must be granted a specific role by system or program administrators to conduct their work in the system.

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?

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 electronic copy, in the system, as needed for reference.

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

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

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 risk to the individual is very low. While data is retained in the system, only authorized individuals have access to the system. User access to the system will be role and least-privilege based.

There is a risk that contact information will become out of date based on seven years of storage. It is expected that additional correspondence from individuals will allow for the system to update information so it is consistent.

Additionally, 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.

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?

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.

4.2 How is the information transmitted or disclosed?

The information will be transmitted using services established in the system security boundary including Microsoft Dynamics 365, Microsoft Office 365 Multi-Tenant's services, and Microsoft Azure for Government Virtual Machines. 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.

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.

The privacy risks associated with the internal information sharing are low. There is a risk that information received by the system will be shared by approved users to others that may or may not have a business need. This includes the ability to look up contact information to send correspondence responses as well as print hard copies of correspondence and contact information to facilitate the sending of said responses. This 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.

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?

No sharing of information with external organizations is expected beyond that sending of correspondence responses to individuals and organizations that have requested a response. This will be done by USDA individuals outside of the scope of the information technology system. Information from the system may be requested under the Freedom of Information Act (FOIA), and if so, appropriate redactions will be made to prevent release of PII.

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 System of Records Notice (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 Department does not intend to share PII or other data outside the Department, except as documented in the routine uses described in the System of Record Notice (SORN).

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

Not applicable. The Department does not intend to share PII or other data outside the Department.

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

There are no anticipated risks as PII information and other data will not be shared outside the Department. Microsoft employees supporting the Dynamics, Office 365, and Azure platforms do not have access to the data stored within government customer instances and cannot access it without express permissions granted by government managed global administrators.

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 System of Records Notice (SORN) and if so, please provide SORN name and URL.

Yes. SORN name and URL not established/updated yet for updated system. There is a SORN published for a previously developed version of this system at:

https://www.federalregister.gov/documents/2014/03/12/2014-05351/privacy-act-of-1974-deletion-of-system-of-records-usdaoes-1-correspondence-and-document-management#page-13979 under the system name: USDA Correspondence and Document Management System (CDMS) USDA/OES-02.

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

As information is voluntarily provided to the Department from unknown sources, there is no ability to provide notice to individuals prior to receipt of said information beyond the aforementioned SORN.

All USDA users will only access the application from a USDA provided machine and will see the standard government access warning upon authenticating to their system and Active Directory account.

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

As information is voluntarily provided to the Department from unknown sources, this question is not applicable because there is no request from USDA to have information be declined.

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

If individuals would like personal information to be used in a particular fashion, then it should be included in whatever correspondence is sent to the Department as an additional handling instruction. System users will be able to handle received information as needed based on said instructions.

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 will be provided through a SORN posted to the Federal Register. The risk is that an individual will not fully understand how their information could be used despite it being voluntarily provided. The system has mitigations in place to limit the exposure of information as described in previous sections. A regular Privacy Act Notice to individuals submitting information is not provided given that individuals submit correspondence to the Department voluntarily and do not have access to the system. Information is not submitted directly to the system.

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 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

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 folder, 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 Director, OES can be obtained from the USDA web site. The OES Director's contact information is detailed in the SORN. Individuals can contact the OES Director and request that the system manager correct any inaccurate information in the system.

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

Contact information for the Director, Office of Executive Secretariat can be obtained from the USDA web site. Individuals can contact the OES Director and request that the system manager correct any inaccurate information in the system

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

The risk is that individuals who want to conduct redress will not know where to find the appropriate SORN to communicate to the Department in the proper manner. This is mitigated by designing the procedures in such a way that is similar to the regular processing of correspondence. As a result, the method to conduct redress is the same method an individual would use to communicate to the Department in the first place.

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?

Only users that have enabled USDA Active Directory credentials, have access to the USDA network will be able to access the system.

This system uses role-based access control to assign privileges to users of the system. Access to the data will be determined through specified role-based permissions as authorized by the system owner. These role-based access controls limit access to ABE based upon the principal of least privilege. The principal 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 ABE, allocates 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 OES application administrators. Only users responsible for processing Secretarial correspondence and other controlled correspondence will be granted access to the system. OES staff with the appropriate permissions will authorize users to access the system. User requests will be confirmed and passed to the Client Experience Center to receive a license and be added to the appropriate Active Directory group. Once completed, The Dynamics System Administrator in OES will assign the respective permissions commensurate with the user's role in the system.

8.2 Will Department contractors have access to the system?

Yes, a limited number of Department contractors will have access to the system to support the administration and management of its functions and security. These users are required to obtain a USDA network account and abide by all Department security and privacy requirements as

defined by NIST standards. In addition, contractors supporting and accessing this system will be required to take annual Information Security Awareness and Rules of Behavior training

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

Users are expected to complete the standard USDA privacy and security training required to maintain their USDA network accounts. There is no additional system specific privacy training expected that is not already covered by the aforementioned training.

8.4 Has Certification & Accreditation (C&A) been completed for the system or systems supporting the program?

The system is currently undergoing development, and C&A information is currently being developed. Microsoft Dynamics 365, Microsoft Office 365 Multi-Tenant (MT), USDA Enterprise Active Directory (EAD), and USDA – CEC Client Services have all received Authority to Operate (ATO) by the USDA CIO. Microsoft Azure for Government is pending an ATO from USDA. The system will leverage virtual machines provided by CEC's Client Services before moving to Azure for Government once the full ATO has been received. Dynamics 365, Office 365 MT, and Azure for Government have received FedRAMP ATOs.

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

Microsoft Dynamics 365 will provide auditing on record access by system users. It is expected that the system will inherit auditing measures established by inheritable services across Office 365 MT and Azure for Government. These auditing measures can be reviewed in their appropriate system ATOs.

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?

As with any correspondence tracking system, there is a risk that malicious or inadvertent actions taken on a particular correspondence may not be traceable back to an individual. This risk is mitigated within ABE by auditing controls in Dynamics 365 whereby actions taken by a user on a package are tracked. This auditing feature maintains accountability of an action taken by an authorized user.

There is a risk with ABE of an authorized individual having more permissions than required to perform their job function. This risk exists when any new user account is created. To counter this risk, the OES staff is responsible for reviewing the system permission matrix to ensure that individual users are only granted the permissions that they are authorized to hold and for which

they have an authorized need; and there are no unauthorized individuals with access to the system.

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 system is an information technology, cloud-based Customer Relationship Management (CRM) system customized with business centric workflows and metadata to support the receipt, processing, and storage or Department received correspondence.

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

The technology used is FedRAMP approved, and we do not expect that they would raise privacy concerns based on their common usage and established authority to operate by multiple Federal entities including FedRAMP.

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. Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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?

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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?

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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 as no public users are expected to access this system. It is wholly contained within USDA network access.

10.10 Does the system use web measurement and customization technology?

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

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 as no public users are expected to access this system. It is wholly contained within USDA network access.

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.

Not applicable as no public users are expected to access this system. It is wholly contained within USDA network access.

Responsible Officials

JOSEPH KOSS Digitally signed by JOSEPH KOSS Date: 2018.09.25 16:01:22 -04'00'

Joe Koss
Office of the Executive Secretariat (OES)
Office of the Secretary of Agriculture (OSEC)

LOUREATH A GIBSON Digitally signed by LOUREATHA GIBSON Date: 2018.09.25 16:04:05 -04'00'

Louretha Gibson
ISSPM
Office of the Executive Secretariat (OES)
Office of the Secretary of Agriculture (OSEC)

Approval Signature

JEAN DANIEL Digitally signed by JEAN DANIEL Date: 2018.09.26 10:51:22 -04'00'

Jean Daniel
Director, OES
Office of the Executive Secretariat (OES)
Office of the Secretary of Agriculture (OSEC)