Privacy Impact Assessment Workiva

Office of the Chief Financial Officer

- Version: 1.0
- Date: January 13, 2022
- Prepared for: Office of the Chief Financial Officer-Associate Chief Financial Officer for Shared Systems-Financial Management Services

United States Department of Agriculture

Privacy Impact Assessment for the WORKIVA Wdesk

January 10, 2022

Contact Point

Scott Roy
ACFO-SS-FMS
504-226-3466

Reviewing Official

Kenneth McDuffie
Information System Security Program Manager
USDA ACFO-SS-FMS

(504) 226-3417

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Assistance Chief Financial Officer – Financial Management Systems (ACFO-SS-FMS) Workiva system. The Workiva Wdesk Software as a Service (SaaS) allows customers to collaborate and share documents hosted in the cloud, giving teams the ability to create and edit in real-time from any location. The PIA was conducted because the Workiva Wdesk system stores usda.gov email address which is considered Personally Identifiable Information (PII) within the cloud provided solution.

Overview

System Name: Workiva Wdesk

USDA Component: Office of the Chief Financial Officer

Purpose: ACFO-SS-FMS uses Workiva to collaborate and share documents for the Annual Financial Report. Wdesk is a third party hosted cloud-based solution. Wdesk is hosted outside of the ACFO-SS-FMS boundary. ACFO-SS-FMS currently uses Wdesk to create and connect data and narrative to consolidate and publish financial, performance, and regulatory reports.

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?

Workiva Wdesk collects name, email address, and contact numbers.

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

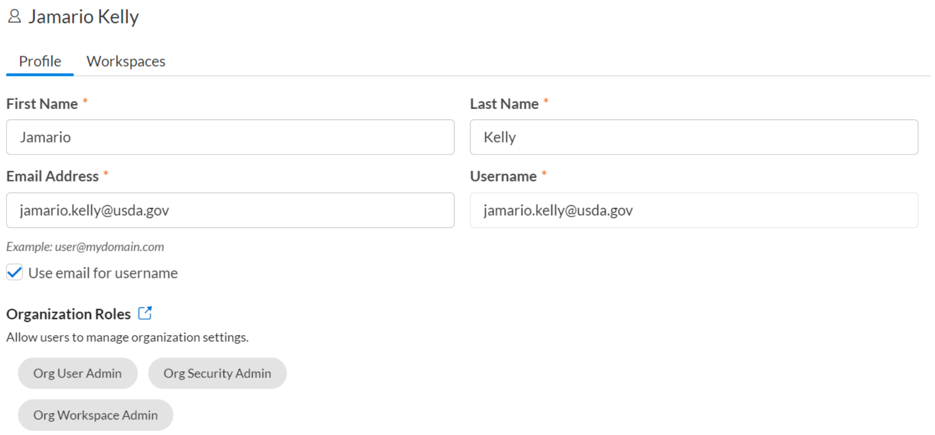
The sources of the information are USDA employees and contractors who use the Workiva Wdesk for data sharing and collaboration.

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

The gathered information is mostly used for account setup for non-PIV users. All information on the document will be publicly accessible data. No, the data used on wDesk will be for the USDA Annual Financial Report. This information contains information that is mandated to be available to the public.

1.4 How is the information collected?

The information is input directly by the users or admins. See example below.



Jamario Kelly

First Name *: Jamario

Last Name *: Kelly

Email Address *: jamario.kelly@usda.gov

Username *: jamario.kelly@usda.gov

Example: user@mydomain.com

☑ Use email for username

Organization Roles

Allow users to manage organization settings.

1.5 How will the information be checked for accuracy?

The data is not checked for accuracy. For eAuthentication (eAuth) related system access and transactions, eAuth does this externally.

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

- **SORN:** USDA/OCIO-2 eAuthentication Service - 82 FR 8503 - January 26, 2017

Legal Authorities:

- 5 U.S.C. Section 301, Departmental regulations.
- 5 U.S.C. Chapter 57, Travel, Transportation, and Subsistence.
- 26 U.S.C. Section 6011, General requirement of return, statement, or list.
- 26 U.S.C Section 6109, Identifying Numbers.
- 31 U.S.C. 3711 through 3719, Claims of the United States Government.

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

- All access to the data in the system is controlled by formal authorization. Each user prior to be given a system account must be approved for the functional roles that are needed within the Workiva Wdesk instance.

- All access to the system is controlled by the eAuthentication application. No actions can be performed in the system without first authenticating.
- Application limits access to relevant information by assigned application functions to roles. This prevents access to unauthorized information.
- The USDA warning banner must be acknowledged prior to application login.
- Annual USDA Security Training must be completed by all USDA employees and contractors.

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 collected is only used for account provisioning.

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

Not Applicable – no special tools in use

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

Not Applicable – system does not use commercial or publicly available data

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.

Workiva Wdesk is protected via USDA eAuthentication which serves as a gateway for accessing the system. Information is protected through various levels of security and policy. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so within the application boundary.

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?

75 Months = 6.25 Years

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

Yes. Records are retained in accordance with NARA policies (OMB/NARA M-12-18). https://www.ocio.usda.gov/policy-directives-records-forms/recordsmanagement/staff-office-file-plan Records Management, USDA DR-3090, Litigation Retention Policy for Documentary Materials including Electronically Stored Information.

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

Assistant Chief Financial Office - Financial Management System (ACFO-FMS) Security division has determined that the data retention periods and practices are adequate to safeguard PII.

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?

Not Applicable. The information is not shared with any external organizations.

4.2 How is the information transmitted or disclosed?

Not Applicable. The information is not shared with any external organizations.

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.

Not Applicable. The information is not shared with any external organizations.

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?

Not Applicable. The information is not shared with any 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.

Not Applicable. The information is not shared with any external organizations.

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

Not Applicable. The information is not shared with any external organizations.

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

Not Applicable. The information is not shared with any 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.

The system is covered under the OCFO-10 SORN.

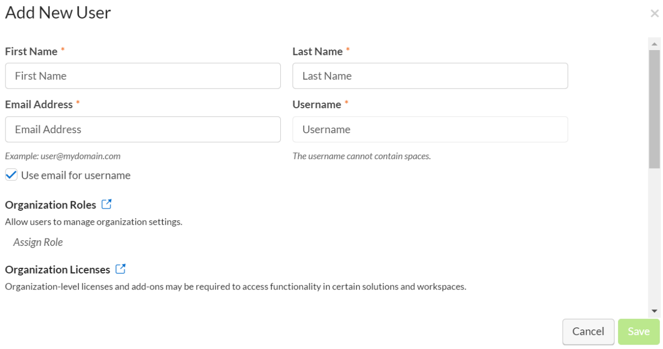
https://www.federalregister.gov/documents/2018/12/31/2018-28375/privacy-act-of1974-system-of-records

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

The U.S. Governments intention to collect PII data is declared in the System of Record Notices, OCFO-10 Financial Systems, made publicly available within the U.S. Federal register, as well as in the Privacy Act, and at data collection points throughout the Federal government. Individuals who enter their own PII data are notified of their rights and protections under the Privacy Act before providing information via those collection points, which are outside the scope of control of USDA ACFO-SS-FMS. If any PII data is provided into Wdesk, it is provided on a voluntary basis directly by the individual into the system or via phone to the helpdesk.

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

No First name, last name, email address and username are mandatory fields for account creation. This information cannot be omitted.



Add New User

First Name *

First Name

Last Name *

Last Name

Email Address *

Email Address

Example: user@mydomain.com

Username *

Username

The username cannot contain spaces.

☑ Use email for username

Organization Roles

Allow users to manage organization settings.

Assign Role

Organization Licenses

Organization-level licenses and add-ons may be required to access functionality in certain solutions and workspaces.

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

User information is not shared outside of the Workiva wDesk internal system.

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

All users who access the Workiva Wdesk application are presented with the standard USDA warning banner that must be acknowledged prior to logging into the system.

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 may obtain information regarding the procedures for gaining access to their own records contained within Workiva Wdesk by submitting a request to the Privacy Act Officer, 1400 Independence Avenue, SW, South Building, Washington, DC 20250. The envelope, and all letters contained therein, should bear the words "Privacy Act Request." A request for information should contain the name of the individual, the individual's correspondence address, the name of the system of records, the year(s) of the records in question, and any other pertinent information to help identify the file(s). This is further explained in SORN OCFO-10, Financial Systems.

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

The user has the option to change personalized information in the profile settings of the system.

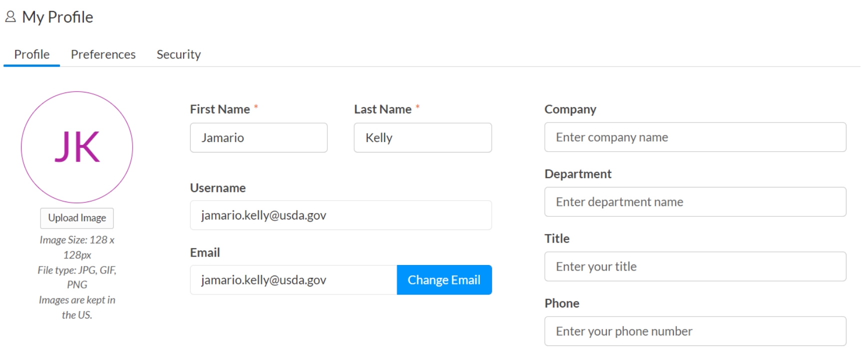


Image Size: 128 x 128px
File type: JPG, GIF, PNG
Images are kept in the US.

First Name * Jamario
Last Name * Kelly
Username jamario.kelly@usda.gov
Email jamario.kelly@usda.gov
Company Enter company name
Department Enter department name
Title Enter your title
Phone Enter your phone number

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

Notification is provided in the system of records notice available in the Federal Register. See OCFO-10, Financial Systems. Procedures for contesting records are the same as procedures for record access in section 7.1 above. Include the reason for contesting the record and the proposed amendment to the information, including any supporting documentation that shows how the record is inaccurate.

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

If formal redress is not possible after contacting USDA in accordance with established procedures, individuals are directed to utilize other legal measures to correct erroneous information, including but not limited, filing civil and/or criminal complaints. See OCFO-10, Financial Systems.

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

Individuals concerned that their PII data may have been compromised may contact the USDA office designated within the System of Records Notice posted in the U.S. Federal Register. See SORN OCFO-10, Financial Systems. Internal employees may also contact their respective Human Resources and/or Privacy Office representative for further assistance.

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?

The system contains automated workflows that can be customized to provide a minimum level of compliant access. This access is based on an individual's relationship with the USDA (i. e. having an identity record in the USDA HR system or Level 2 elevation by Local Registration Authority). Other levels of access can be granted with supervisor approval or approval from a higher-level authority. All access transactions, including approvals, additions, or removals of access are fully logged by the system.

8.2 Will Department contractors have access to the system?

Yes

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

All USDA employees and contractors receive annual security awareness training that includes specific training regarding the protection of PII. Privileged users are required to take additional, more detailed security training commensurate with their access permissions.

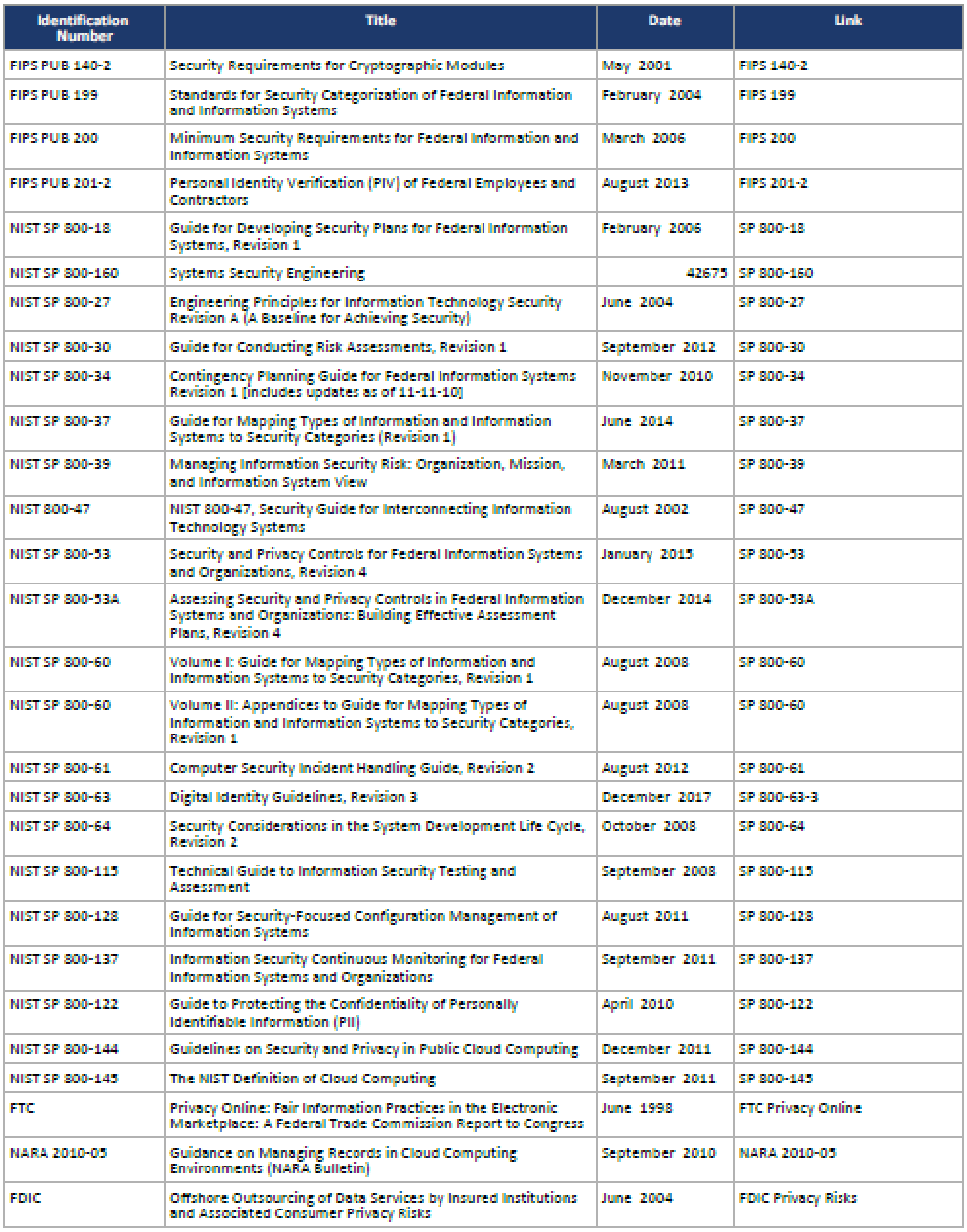
8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

This system is FedRAMP certified.

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

All users are required to have an individual user account to access the system; no temporary or guest accounts are permitted. Auditing is turned on for the system and audit logs are periodically reviewed for indications of misuse. Workiva is a FedRamp certified system and complies with all require technical safeguards to prevent misuse of data. See specific guidelines below captured from Workiva System Security Plan (SSP).

Table 13-8. Workiva Wdesk Standards and Guidance



Identification Number	Title	Date	Link
FIPS PUB 140-2	Security Requirements for Cryptographic Modules	May 2001	FIPS 140-2
FIPS PUB 199	Standards for Security Categorization of Federal Information and Information Systems	February 2004	FIPS 199
FIPS PUB 200	Minimum Security Requirements for Federal Information and Information Systems	March 2006	FIPS 200
FIPS PUB 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors	August 2013	FIPS 201-2
NIST SP 800-18	Guide for Developing Security Plans for Federal Information Systems, Revision 1	February 2006	SP 800-18
NIST SP 800-160	Systems Security Engineering	42675	SP 800-160
NIST SP 800-27	Engineering Principles for Information Technology Security Revision A (A Baseline for Achieving Security)	June 2004	SP 800-27
NIST SP 800-30	Guide for Conducting Risk Assessments, Revision 1	September 2012	SP 800-30
NIST SP 800-34	Contingency Planning Guide for Federal Information Systems Revision 1 (includes updates as of 11-11-10)	November 2010	SP 800-34
NIST SP 800-37	Guide for Mapping Types of Information and Information Systems to Security Categories (Revision 1)	June 2014	SP 800-37
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View	March 2011	SP 800-39
NIST 800-47	NIST 800-47, Security Guide for Interconnecting Information Technology Systems	August 2002	SP 800-47
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4	January 2015	SP 800-53
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Revision 4	December 2014	SP 800-53A
NIST SP 800-60	Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1	August 2008	SP 800-60
NIST SP 800-60	Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1	August 2008	SP 800-60
NIST SP 800-61	Computer Security Incident Handling Guide, Revision 2	August 2012	SP 800-61
NIST SP 800-63	Digital Identity Guidelines, Revision 3	December 2017	SP 800-63-3
NIST SP 800-64	Security Considerations in the System Development Life Cycle, Revision 2	October 2008	SP 800-64
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment	September 2008	SP 800-115
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems	August 2011	SP 800-128
NIST SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations	September 2011	SP 800-137
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	April 2010	SP 800-122
NIST SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing	December 2011	SP 800-144
NIST SP 800-145	The NIST Definition of Cloud Computing	September 2011	SP 800-145
FTC	Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress	June 1998	FTC Privacy Online
NARA 2010-05	Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)	September 2010	NARA 2010-05
FDIC	Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks	June 2004	FDIC Privacy Risks

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?

There are no significant risks associated with the information collected by Workiva Wdesk. There is no data sharing of PII and all personnel accessing the Wdesk system are cleared and trained annually on the proper handling and protection of PII data.

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?

Workiva wDesk is a software as a service (Saas) cloud solution, offering controlled collaboration, data integration, granular permissions and a full audit trail. Wdesk helps mitigate risk, improves productivity and gives users confidence in their data-driven decisions.

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

Wdesk does not use technology that would prompt an increase in concern regarding privacy protection. Workiva Wdesk is FedRamp certified.

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 Wdesk system owner and ISSPM have reviewed both OMB M-10-22 and M-10-23.

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

The use of the Workiva Wdesk enterprise cloud was a result of OMB Memorandum M-12- 10 to shift to commodity IT.

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

No PII will become available through the user of the 3rd party website and application.

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

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

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

Not Applicable

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

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

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

10.10 Does the system use web measurement and customization technology?

Not Applicable

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

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

Responsible Officials

KENNETH MCDUFFIE

Digitally signed by KENNETH MCDUFFIE
Date: 2022.02.08 06:58:28 -06'00'

Kenneth McDuffie
Director, System Security and Compliance Division
Office of the Chief Financial Officer,
Associate Chief Financial Officer for Shared Services
United States Department of Agriculture

Approval Signature

LANCE RAYMOND

Digitally signed by LANCE RAYMOND
Date: 2022.02.14 08:39:26 -06'00'

Lance Raymond, PhD
Director, Financial Management Services
Office of the Chief Financial Officer
Associate Chief Financial Officer for Shared Services
United States Department of Agriculture