USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
04/08/2025	1.0	Reviewed and Updated All pages

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Financial Disclosure Front End (FDOnline)
Program Office	OCIO
Mission Area	DAITO/OE
CSAM Number	2360
Date Submitted for Review	04/08/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Corey Medina	corey.medina@usda.gov	202-573-2810
Information System Security Manager	Lisa McFerson	lisa.McFerson@usda.gov	202-720-8599
System/Program Managers	Andrew Tobin	andrew.tobin@usda.gov	202-720-2251

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

- Define the people who are part of a given business workflow: assigning them roles, permissions, tasks, and responsibilities. FDOnline provides the Office of Ethics with a simple and secure way to collect, review and manage the entire business process of financial disclosures.
- At an application level, the Intelliworx (FDOnline) modules appear as independent web applications with unique URLs and separate logins for each web application. Customers are given access to only the URL and login appropriate for the module they are using.
- The PII within the system is for the inherent purposes of onboarding new hire and filing financial disclosure forms
- Gather information critical to the workflow in a streamlined and intuitive way.
- Map gathered data to official government forms in PDF format
- Define the task that need to be completed by users and provide mechanisms for approvals, notifications/reminders, and reporting.
- Integrate with existing government systems to accept, process and store data.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The Intelliworx (FDonline) application is hosted entirely on the AWS GovCloud Infrastructure-as-a-Service (IaaS) platform, and no hardware or software outside of the AWS GovCloud is used.

At the code level, the Intelliworx platform is a common set of code libraries that allow for the creation of software "modules" that perform specific process automation functions based upon customer requirements. Whether the module purchased by a customer is one that assists in HR processes or one that handles financial disclosure processes, much of the code is the same.

At an application level, the Intelliworx modules (FDOnline) appear as independent web applications with unique URLs and separate logins for each web application. Customers are given access to only the URL and login appropriate for the module they are using.

At the infrastructure level, the Intelliworx Cloud is an environment hosted and secured at AWS GovCloud and consists of a variety of customer modules. The Intelliworx system is a software application platform that allow customer agencies to streamline and automate workflows in any number of mission areas.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

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

5 CFR part 2634

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

Yes, approved 5/15/2025.

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

OGE/GOVT–2 is a system of records containing confidential financial disclosure reports, including OGE Form 450, OGE Optional Form 450-A, and agency supplemental or alternative confidential report forms: https://www.oge.gov/Web/oge.nsf/Resources/OGE+GOVT-2

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

Not Applicable

Section 2: 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

☐ Passport number

☐ License Plate number

☐ Registration number

☐ File/Case ID number

☐ Student ID number

☐ Federal Student Aid number

☐ Employee Identification number

☐ Alien Registration number

☐ DOD ID 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

☐ Health Plan Beneficiary number

☐ Business Mobile number (sole proprietor)

☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)

☐ 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

☐ Religion/Religious Preference

☐ Citizenship

☐ Immigration Status

☐ Home Phone or Fax Number

☒ Home Address

☐ ZIP Code

☐ Marital Status

☐ Spouse Information

☐ Children Information

☐ Military Service Information

☐ Race

☐ Nationality

☐ Mother's Maiden Name

☐ Personal Email Address

☐ Business Email Address

☐ Global Positioning System (GPS)/Location Data

☐ Employment Information

☐ Alias (Username/Screenname)

☐ Personal Financial Information (Including loan information)

☐ Education Information

☐ Resume or Curriculum Vitae

☐ Business Financial Information (Including loan information)

☐ Professional/Personal References

Biometrics

☐ Fingerprints

☐ Hair Color

☐ DNA Sample or Profile

☐ Retina/Iris Scans

☐ Video Recording

Distinguishing Features

☐ Palm Prints
☐ Dental Profile
☐ Eye Color
☐ Photos
☐ Signatures

Characteristics

☐ Vascular Scans
☐ Scars, Marks, Tattoos
☐ Height
☐ Voice/Audio Recording
☐ Weight

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)
☐ Cell Tower Records (e.g., Logs, User Location, Time)
☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information
☐ Workers' Compensation Information
☐ Mental Health Information
☐ Patient ID Number
☐ Disability Information
☐ Emergency Contact Information

Specific Information/File Types

☐ Personnel Files
☐ Health Information
☐ Case Files
☐ Law Enforcement Information
☐ Academic/Professional Background Information
☐ Security Clearance/Background Check
☐ Credit History Information
☐ Civil/Criminal History Information/Police Record
☐ Taxpayer Information/Tax Return Information

- Demographics (race, nationality, ethnicity) Employment
- Work address
- Grade
- Title work phone Types
- Amounts of salaries, investments
- Assets Creditor name, city, state, country

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

The Intelliworx system collects PII within the following fields for the inherent purposes of onboarding new hires and filing financials disclosure forms. The PII is integral to the business processes of the Intelliworx system.

- Full Name
- Date of Birth
- Social Security Number
- Home Address
- Telephone number
- Email address
- Demographics (race, nationality, ethnicity)
- Employment: work address grade, title
- work phone Types and amounts of salaries
- investments
- and assets Creditor name, city, state, country

2.2.1. How is the information collected?

The PII is considered to be current as it is entered directly by the individual at the time of onboarding or filing. Individuals are responsible for entering accurate PII and maintaining accurate data submitted.

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

No

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

In addition to automated formatting validation within the software, HRworx verifies bank routing numbers within the onboarding module against the Federal Reserve FedACH routing directory.

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

Yes

2.5.1. Does the system/program use third-party websites? What is the purpose of the use of third-party websites?

The Onboarding module sends required PII (basic personal details, tax information) to the USDA's National Finance Center (NFC) EmpowHR system for payroll purposes.

The FDonline module does not provide PII to any third-party organizations.

Customers of the Intelliworx system establish the criteria for granting system account access to the PII managed by the customer. The Onboarding module transmit required PII (basic personal details, tax information) to the USDA's National Finance Center (NFC) empowHR system for payroll purposes.

The FDonline module does not provide PII to any third-party organizations or agency or mission.

Customers of the Intelliworx system establish the criteria for granting system account access to the PII managed by the customer or USDA's programs.

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

The Onboarding module sends required PII (basic personal details, tax information) to the USDA's National Finance Center (NFC) EmpowHR system for payroll purposes

2.6. **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: By Implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

Section 3: 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?

The Intelliworx system gather PII information in certain fields to facilitate the onboarding of the new employees and completion of financials disclosure forms, aligning with the systems intended purpose and confirming the business scope.

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.

No

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Mitigation: By Implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Section 4: 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?

Federal agency customers populating the system with PII is integral to the business processes of the Intelliworx system. HRworx only populates the Intelliworx system with PII during the initial onboarding of customers, if the federal agency provides the data to be loaded into the system.

The PII is integral to the business processes of the Intelliworx system

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

Within the FDonline module, individuals are not able to opt-out of providing PII or consent to only a particular use. The PII collected and used is required by the Office of Government Ethics (OGE). Declining to provide PII effectively declines employment.

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: **Privacy Act risks associated with notices include:**

Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Non-compliance with Regulations: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

User Consent: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Section 5: 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?

Once data has reached the six (6) year maximum retention period within FDonline, records are moved to a queue where customers (e.g., data owners) must designate whether the record can be purged or if the record needs to be held.

Once data within the onboarding module has reached the end of the ninety (90) day retention period, it is automatically purged from the system, as long as certain conditions are met (e.g., the process cannot be ongoing).

The Intelliworx system does not maintain reports that contain PII as there is no need or business process that necessitates this.

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.

In accordance with the National Archives and Records Administration General Records Schedule 2.8 Employee Ethics Records, these records generally are retained for six years after filing, except when filed by or with respect to a nominee and the nominee ceases to be under consideration for the position. However, if any records are needed in an ongoing investigation, they will be retained until no longer needed in the investigation. Destruction is by shredding or electronic deletion.

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the retention of information include:

Excessive Data Retention: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

Data Breaches: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Non-compliance with Regulations: Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.

Mitigation: By implementing the following mitigation actions, mission areas can ensure responsible retention of PII while complying with the PA.

Data Retention Policy: Use NARA data retention policies that outlines how long different types of PII will be retained and the rationale for those timeframes.

Regular Reviews: Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.

Secure Disposal Procedures: Establish secure methods for the disposal of personal information that is no longer needed, such as shredding paper documents or using data-wiping software for electronic files.

Section 6: 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?

The Onboarding module sends required PII (basic personal details, tax information) to the USDA's National Finance Center (NFC) EmpowHR system for payroll purposes.

The FDonline module does not provide PII to any third-party organizations.

Customers of the Intelliworx system establish the criteria for granting system account access to the PII managed by the customer.

Federal agency customers populating the system with PII is integral to the business processes of the Intelliworx system. HRworx only populates the Intelliworx system with PII during the initial onboarding of customers, if the federal agency provides the data to be loaded into the system.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Privacy risks associated with internal sharing and disclosure include:

Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

Data Breaches: Internal systems can be vulnerable to breaches, compromising PII.

Insider Threats: Employees with malicious intent may exploit their access to PII for personal gain.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Access Controls: Implement role-based access controls to limit who can access PII based on their job responsibilities.

Encryption: Use encryption for data in transit and at rest to protect PII from unauthorized access.

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?

The PII is integral to the business processes of the Intelliworx system.

The FDonline module does not provide PII to any third-party organizations.

Customers of the Intelliworx system establish the criteria for granting system account access to the PII managed by the customer.

6.4. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: **Privacy risks associated with external sharing and disclosure include:**

Unauthorized Access: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Data Breaches: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Loss of Control: Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Data Sharing Policy: Develop a clear policy outlining the conditions under which PII can be shared externally, including legal and compliance requirements (ex.: Computer Matching Agreements, SORNs, Business Agreements).

Due Diligence: Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.

Written Agreements: Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.

Section 7: 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?

New hires have the ability to login to the Onboarding module, review the PII that is being maintained, and update their PII throughout the onboarding process.

Filers within the FDonline module are required to update their PII on an annual basis when reporting their financial assets. Individual filers can work with the agency's designated ethics administrators to request access to their records and reopen a filing if PII needs to be updated for the current filing year.

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

In addition to automated formatting validation within the software, HRworx verifies bank routing numbers within the onboarding module against the Federal Reserve FedACH routing directory.

It is required of the agency to implement processes that verify accuracy of the PII collected.

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

New hires have the ability to login to the Onboarding module, review the PII that is being maintained, and update their PII throughout the onboarding process.

Filers within the FDonline module are required to update their PII on an annual basis when reporting their financial assets. Individual filers can work with the agency's designated ethics administrators to request access to their records and reopen a filing if PII needs to be updated for the current filing year.

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

The PII is considered to be current as it is entered directly by the individual at the time of onboarding or filing. Individuals are responsible for entering accurate PII and maintaining currency of the data submitted.

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

Privacy Risk: Privacy Act risks associated with redress include:

Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Failure to Address Complaints: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

Mitigation: By implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

Dedicated Privacy Officer/Privacy Point of Contact: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

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?

The system uses Multi-factor Authentication (MFA) and Role Base Access Control (RBAC) with end- to- end encryption.

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

The FDonline administrator and program federal lead must authorize a ticket request before granting user access. The ATO includes documentation of all procedures.

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

Not Applicable.

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

Annual government training for all government employees/ Contractors must be completed.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 5/22/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

Signed:TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.07.02 04:08:50 -04'00'

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed:______________________________________

Andrew Tobin
System Owner
U.S. Department of Agriculture

Signed:______________________________________

Corey Medina
Mission Area Privacy Officer
U.S. Department of Agriculture

Signed:______________________________________

Office of the Chief Privacy Officer
U.S. Department of Agriculture