U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

U.S. DEPARTMENT OF AGRICULTURE

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 for the USDA IT System/Project:

Iron Mountain Digital Record Center for Images (DRCI)

OCFO -National Finance Center (NFC)

DAITO

Date PIA submitted for review:

11/20/2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	*Michele Washington*	*michele.washington@usda.gov*	*202-205-3369*
Information System Security Manager	*Tracy Haskins*	*tracy.haskins@usda.gov*	*202-720-8245*
System/Program Managers	*Trudy Sandefer*	*trudy.sandefer@usda.gov*	*202-258-2254*

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

The Digital Records Center for Images is a contractor system owned by Iron Mountain. The system provides document storage of legacy paper and microfiche records, as well as line-data feeds for the USDA National Finance Center. Employee and contractor Personally Identifiable Information is contained within the records.

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 Digital Record Center for Images (DRCI) is owned and operated by the Information Governance Digital Solutions ("IGDS") division of Iron Mountain. DRCI is used to provide an online web-based archive and retrieval system for line-data feeds as well as legacy microfiche and microfilm that has been converted to digital images, to the United States federal departments. IGDS provides an isolated instance of its DRCI for USDA, which supports COLD data, images, and PDFs. The system consists of web servers, Kofax systems used to scan and store digital files, a Van Dyke system to securely transfer data, and Alfresco Enterprise Content Management Service for search and retrieval functionality. Iron Mountain has legal authority and appropriate licensing to operate the system.

Section 1.0 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?

USDA's authorization to collect information is allowed by:
Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998
Federal Register Nol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations

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

Authority to Operate (ATO) Date: June 9, 2023
ATO Expiration Date: December 31, 2023

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

SORN-OCFO 1 Systems for Personnel, Payroll, and Time & Attendance

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

Yes, the collection of information is covered by the Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998

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)	☐	Sex	☐	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?

The system's data is sourced from:

- Administrative Billings and Collections System (ABCO), CSAM ID: 1035
- Direct Premium Remittance System (DPRS), CSAM ID: 1036
- Payroll Accounting System (PAS), CSAM ID: 1045
- Payroll/Personnel System (PPS), CSAM ID: 1046

2.2.1. How is the information collected?

Documents are picked up or shipped from the federal agencies' offices via a secure monitored transport method to designated Iron Mountain scanning facilities. They are then scanned, indexed, and loaded for viewing within 48 hours. Line-data is transferred over a secure VPN to an SFTP site, converted to PDF, and loaded into the DRCI for viewing within 24 hours.

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

N/A

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

The accuracy of the data is handled by the USDA per their standard operating procedures. DRCI does not perform accuracy checks of line data contents. Any files received that cannot be identified by report contents (file names. header info, etc.) will be rejected and notifications sent. Scanned records have validation/verification procedures when entering metadata.

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

N/A. No third-party websites or applications are being used.

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

N/A. No third-party websites or applications are being used.

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

N/A. No third-party websites or applications are being used.

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of 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.

User Consent for Sensitive Data: Obtain explicit consent for the collection and processing of sensitive personal information, such as health or financial data, and ensure that users are aware of its characterization.

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?

DRCI is a web-based, hosted image repository used to store and manage any type of electronic document or record. Users can store electronic documents with confidence, knowing that their important corporate information is always safe and secure, yet quickly accessible by authorized users when needed. The clients can request on demand imaging of the stored legacy microfiche and microfilm 24x7x366. The media is retrieved by designated staff with clearance. The media is retrieved from storage, converted to digital image and uploaded for viewing by the close of business the next business day. Information Governance Digital Solutions ("IGDS") is a division of Iron Mountain which offers paper to digital and digital to digital transformation and storage of documents which can then be viewed in digital form. DRCI is an implementation of the following technologies specifically for the Federal Government Digital Record Center for Images (DRCI) is used to provide an online web-based archive and retrieval system for line data feeds in PDF format and legacy microfiche and microfilm which have been converted to digital images, to the United States federal departments. IGDS provides an isolated instance of its DRCI for USDA, which supports data, images, and PDF's. Kofax Central (Kofax) is used for conversion of paper documents to digital. Isolated instances of Kofax are utilized for FDS. The service also provides capability to pick up paper documents from the federal agencies offices via a secure monitored transport method and have them scanned, indexed and loaded for viewing within 48 hours. The digital images of the documents are in a secure single chain of custody throughout the process. Data and folders containing digital images are encrypted using Vormetric, Isilon and CTERA encryption.
DRCI, is a Web Based solution accessible to users and administrators with capabilities based on their individual roles and responsibilities and administrative privileges via a web browser. It does not

require installation of any client software or update to client systems or client-side browser or system configuration. Users accessing DRCI can only access the information they have been authorized to view, edit or share all other information, such as documents, files, folders, etc. are not visible to the user. All user privileges are restricted based on the document security assignments for functions such as updating metadata and adding annotation notes. This level of access controls significantly lowers the security risk for the entire system.

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.

Iron Mountain maintains a centralized monitoring tool that alerts specified personnel to incidents concerning the security stature of the environment. The Chronicle SIEM tool takes critical information from outputs of technology platforms such as Crowd Strike, Tenable, and Tanium. These tools provide critical information that the Cybersecurity Incident Response Team uses to triage incidents to follow the procedures outlined in the Cybersecurity Incident Response Plan.

Iron Mountain has placed information security devices at critical points in the network infrastructure to check for anomalies traffic. There are Intrusion Prevention Systems, Intrusion Detection System and firewalls architected in accordance with the Company Secure Engineering and Architecture Principles Standard which is approved and reviewed by the CISO.

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 4.0 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?

SORN-OCFO/NFC 1 Systems for Personnel, Payroll, and Time & Attendance

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

N/A. The system's data is sourced from other information systems.

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.

Insufficient Updates: Notices that are not regularly updated to reflect changes in data practices or legal requirements can mislead individuals and result in privacy violations.

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.

Transparency: Clearly outline what personal data is being collected, the purpose of data collection, how it will be used, and who it will be shared with.

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?

Data will be maintained according to the individual customer's retention policy DR 3090-001.

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.

Data will be maintained according to the individual customer's retention.

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: 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.

Access Controls: Implement strict access controls to limit who can view and manage retained personal information, reducing the risk of unauthorized access.

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?

Iron Mountain does not share any data internally. Internal data is shared within NFC is known only to IM based on system logging of user activity in the DRCI. Use within NFC is known only to IM based on system logging of user activity in the DRCI. Internal IM users do not share or send information within the organization.

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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?

PII is not shared with any external organization.

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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

Individuals seeking to contest or amend information maintained in the system should direct their request to the listed NFC Director below and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address including zip code, name of the system of records, year of records in question, and any other pertinent information to help identify the data requested.

Director, National Finance Center, 13800 Old Gentilly Road, Building 318, New Orleans, LA 70129, nfc.1.sorn@ usda.gov, 504–426–0120.

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

SORN-OCFO 1 Systems for Personnel, Payroll, and Time & Attendance

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

N/A

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: 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.

Timely Response Protocols: Implement protocols for acknowledging and responding to redress requests promptly, ensuring that individuals feel heard and valued.

Investigation Processes: Create structured process for investigating redress requests, including gathering necessary information and documenting findings.

Remediation Options: Offer various remediation options, such as data correction, deletion, or

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?

Verification of authorized users is conducted quarterly by Iron Mountain. Only authorized users can maintain access. All user actions are logged and audit-able upon request.

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

All data is encrypted. Access is strictly controlled by role-based access control.

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

Iron Mountain does not share any data internally or externally.

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

All IRM employees with access to Iron Mountain's IT infrastructure take Iron Mountain's global privacy and/or global information security training on a yearly basis.