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
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Insight
Program Office	OCFO, Nation al Finance Center
Mission Area	Web Applications Directorate/Payroll Web Systems Branch
CSAM Number	
Date Submitted for Review	

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Michele A. Washington	Michele.washington@usda.gov	202-577-8021
Information System Security Manager	Tracy Haskins	Tracy.haskins@usda.gov	202-720-8245
System/Program Managers	Renee Pellissier	Renee.Pellisier@usda.gov	318-401-5850

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 information system is the National Finance Center (NFC) Insight, providing human resource reports. Insight contains Human Resource (HR) Privacy Identification Information (PII).

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.

Insight provides workforce information with metrics and attributes to allow Human Resources (HR) to analyze workforce staffing and productivity. Management uses the reports to monitor workforce, such as time and attendance, leave, and tracking projects. Data for analysis is provided via system generated reports and ad hoc queries for client organizations using information originating from the Payroll/Personnel System (PPS), EmpowHR, and Administrative Billings and Collections System (ABCO).

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?

The legal authorities for USDA to collect, maintain, use, and disseminate information, includes:

1. Financial Systems is the Chief Financial Officers Act of 1990 (Pub. L. 101–576)
2. eCFR Title 7, Agriculture, Subtitle B

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

Yes, 12/31/2024.

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

The SORN is OCFO/NFC-1 Office of the Chief Financial Officer (OCFO), National Finance Center (NFC).

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

No

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	☐ Eye Color	☐ Signatures
☐ Dental Profile	☐ Photos	

Characteristics

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

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

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 source information originates from the Payroll/Personnel System (PPS), EmpowHR, and Administrative Billings and Collections System (ABCO).

2.2.1. How is the information collected?

Source information within flat files is transmitted via secure SFTP and loaded into the Insight database.

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; commercial or publicly available data is not used.

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

Insight data reflects what is in the source system and is not changed.

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

No

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

N/A

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

No Insight PII is available through the use of third-party websites/applications.

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.

Non-compliance with Regulations: Failing to accurately characterize information can lead to non-compliance with privacy laws and regulations, resulting in legal penalties and reputational damage.

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

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 source information originates from the Payroll/Personnel System (PPS), EmpowHR, and Administrative Billings and Collections System (ABCO). The system provides workforce information with metrics and attributes to allow HR to analyze workforce staffing and productivity.

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 risks may 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.

Overuse of Information: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Loss of Data Control: When PII is shared with third parties, there is a risk of losing control over how that data is used, potentially leading to unauthorized access or exploitation.

Increased Risk of Data Breaches: The more PII is used and shared, the higher the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

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

Purpose Limitation: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

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?

Notice is provided during normal HR new hire processes for all federal employees, and included in the SORN, OCFO/NFC-1.

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

Information is gathered as part of the normal hiring activity for all federal employees and required to provide compensation and benefits to the employee.

Individuals have the opportunity to decline to provide the information and are informed that the data is required to complete routine business functions.

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: Data Retention

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

5.1. What information is retained and for how long?

The systems consist of current and historical personnel, payroll, time and attendance, and debt collection records for NFC's customers, which are retained for 56 years.

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.

Yes, Agency Record Control Schedule N1-016-10-7 is approved.

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 outline 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 source data is loaded into the Insight database and not subsequently shared, transmitted, or exported to any other internal applications or internal organizations; except to be viewed by the federal agency which owns and originally provided the data. Insight provides reporting information to allow HR to analyze workforce staffing and productivity.

Source information within flat files is transmitted using standard FTP over USDA encrypted Virtual Private Network (VPN) tunnel between NFC and NITC data centers and loaded into the database. Reporting information is disclosed via secure Oracle HTTPS Server (OHS) based web access to authorized users requiring a valid user identification and password to access Insight.

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

Follow the format below:

Privacy Risk: Unauthorized disclosure of salary, health benefit deduction, health benefits, social security number or bank account could adversely affect employees of USDA.

Mitigation: Source data comes into Insight from three internal NFC applications under the same Authorizing Official (AO). The internal systems have been authorized to operate and follow USDA Risk Management Framework guidelines, processes and procedures which are compliant to OMB directives, FISMA and NIST requirements.

NFC personnel go through NACI background checks and receive annual security awareness training with the Rules of Behavior required acknowledgement. Source information within flat files is transmitted via secure file transfer protocol (SFTP) over USDA encrypted Virtual Private Network (VPN) tunnel between NFC and NITC data centers and loaded into the database. Reporting information is disclosed via secure Oracle HTTPS Server (OHS) based web access to authorized users requiring a valid user identification and password to access Insight.

The database is not accessible by web interface user. Physical access to the database is restricted through automated mechanisms to recognize potential intrusions, which include video monitoring and recording, badge readers, biometric scanners, and audible alarms.

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?

Insight does not export or transmit data to any external organizations or other applications. The source data is loaded into the Insight database and not subsequently shared with any other external applications or external organizations; except to be viewed by the federal agency which owns and originally provided the data. Insight stores federal agencies' workforce information and provides reporting capabilities that allows federal agencies' HR staff to analyze their agency's workforce staffing and productivity data. Organizations are only allowed to view their own agency's information, at the level of their account, approved by their agency, based on least privilege.

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

Follow the format below:

Privacy Risk: N/A. Insight does not export or transmit data to any external organizations or other applications.

Mitigation: N/A. Insight does not export or transmit data to any external organizations or other applications.

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?

Procedures for Individual redress are outlined in the SORN OCFO/NFC-1 for Payroll/Personnel System.

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

Individuals would contact their HR representative, and the corrections would be made within the source Payroll/Personnel System.

Additionally, procedures to correct information in the source system are outlined in SORN OCFO/NFC-1 for Payroll/Personnel System which are as follow:

Notification procedure: Employees may request information from this system from the appropriate personnel office having custody of his/her records. A request for information should be addressed to the Director, Personnel Division (name of appropriate Agency), USDA, at the address shown under Location and should contain the name of requestor, employing agency in USDA or agency to which information was furnished, address of agency and particular information requested.

Record access procedures: Any individual may obtain information as to the procedures for gaining access to and contesting a record in the system which pertains to him/her by submitting a written request to the appropriate office referred to in the preceding paragraph. Contesting record procedures: Same as Record access procedures.

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

SORN OCFO/NFC-1 for Payroll/Personnel System: Notification procedure: Employees may request information from this system from the appropriate personnel office having custody of his/her records. A request for information should be addressed to the Director, Personnel Division (name of appropriate Agency), USDA, at the address shown under Location and should contain the name of requestor, employing agency in USDA or agency to which information was furnished, address of agency and particular information requested.

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

There are no alternatives available through Insight. The redress would be through the source systems.

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 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.

Individuals can request access, correction or amendment of their records contained in Insight by contacting the official for the office managing the Payroll Personnel system:

National Finance Center, Director, 13800 Old Gentilly Road, building 318, New Orleans, LA 70129, email NFC.1.SORN@usda.gov or call 504–426–0120.—For Privacy Act questions concerning this revised system of records notice, please contact USDA Departmental Administration Information Technology Office, Office of the Chief Information Officer, United States

Department of Agriculture, email at: ocio.cio.daitoservices@usda.gov, or by phone at: 202–577–8071. —For general USDA Privacy Act questions, please contact the USDA Chief Privacy Officer, Information Security Center, Office of the Chief Information Officer, USDA, Jamie L. Whitten Building, 100 Independence Ave. SW, Washington, DC 20250, email: USDAprivacy@usda.gov.

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?

DISC hosts Insight. The operating system tracks system specific information, such as databases, antivirus, and application-level events as determined by the COTS software. Oracle tracks SYS account login activity. Access to the database is only provided by system administrators with privileged accounts. Users do not have access to the database. Physical access to the database is restricted through automated mechanisms to recognize potential intrusions, which include video monitoring and recording, badge readers, biometric scanners, and audible alarms.

The application is controlled by security attributes which only allow authorized users to access the system. The hosting environment also provides technical safeguards, such as database encryption, to prevent misuse of data.

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

The agencies determine user access. NFC follows Title VII, Chapter 11, Directive 2, Access Management, and Directive 58, Information Systems Security Program. User account creation goes through a defined process for any access to any system within NFC. The end users' agency security officers (ASOs) submit a request to the NFC Access Management Branch to add users in a defined role. Procedures are documented within NFC. The ASOs are the point of contact between the system users and CPOC Access Management Branch. The ASOs are responsible for ensuring that Insight users have completed the required training (e.g., PII, SAT, ROB) and clearance process prior to requesting access for these users. This applies to all federal employees.

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

The program has established a robust process for reviewing and approving information sharing activities to ensure compliance with privacy regulations and safeguard the privacy of individuals' information. The following statement outlines the key elements of this process:

Regular Privacy Impact Assessment (PIA) Reviews:
The program conducts regular Privacy Impact Assessments to identify and evaluate privacy risks associated with information sharing activities.
These assessments consider the sensitivity and scope of the collected information and assess any potential privacy risks arising from information sharing within and outside the program.

Security Control Documentation and Testing:
A comprehensive System Security Plan (SSP) is in place, documenting the security controls implemented to protect shared information.
These security controls are tested annually through continuous monitoring, SSAE 18, and A-123 programs to validate their effectiveness.

Training and Awareness:
The program provides privacy and Personally Identifiable Information (PII) training to all users, including federal employees and contractors.
This training ensures that individuals involved in information sharing activities are aware of their responsibilities and understand the implications of privacy.

Training materials cover topics such as security awareness, rules of behavior, privacy, best practices, and protection of sensitive information.
Role-Based Access and Least Privilege Principle:
Access to the system and shared information follows the principle of the least privilege, granting users the minimum necessary access rights based on their roles and responsibilities.

Access requests are reviewed and determined by designated personnel/payroll agency security officers and authorized by the appropriate authorities.
The Office of the Chief Information Officer/Information Security Center/Information Technology Service Center/Access Management Branch manages the granting of access to individual users.

Encryption and Data Protection Measures:
The program employs encryption protocols to safeguard shared data both in motion and at rest.
Data is encrypted when shared within the USDA network to protect against unauthorized access.
Contractors and external parties accessing the system are required to adhere to encryption protocols to ensure that Personally Identifiable Information (PII) is not shared in an unencrypted format.

Ongoing Monitoring and Compliance:
The program maintains a continuous monitoring process to track and assess information sharing activities.
Compliance with privacy regulations, security controls, and data protection measures is regularly reviewed to ensure ongoing adherence and effectiveness.

Through these measures, the program ensures that information sharing is conducted in a privacy-conscious manner. By conducting regular assessments, implementing robust security controls, providing training, and enforcing access restrictions, the program strives to protect the privacy of individuals' information and maintain compliance with applicable privacy laws and regulations.

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

Privacy and PII training are included in the Security Awareness and Rules of Behavior training that is required for all federal employees and contractors annually. An exam is provided following the training, and the user must receive 70% or better to maintain or receive access to the information system. Some NFC staff members receive additional privacy training according to their role within NFC.