

Privacy Impact Assessment

EmpowHR - Human Capital Management System

- Version: 3.2
- Date: August 31, 2023
- Prepared for: USDA, OCFO, National Finance Center





Privacy Impact Assessment for the Human Capital Management System (EmpowHR)

August 31, 2023

Contact Point

Trudy Sandefer
OCFO, National Finance Center
504-426-7663

Reviewing Official

Tracy Haskins
Information System Security Manager
United States Department of Agriculture
202-720-8245

Abstract

The National Finance Center (NFC) is a Shared Service Center (SSC) under the Office of Personnel Management Human Resources Line of Business (HRLOB). The Human Capital Management System offering, EmpowHR, is a web based human resources information system. EmpowHR allows the United States Department of Agriculture (USDA) and its customers to access employment information from a centralized database maintained by their human resources departments. This Privacy Impact Assessment (PIA) is being conducted to fulfill the requirements of Section 208 of Public Law 107-347 (the E- Government Act of 2002).

Overview

EmpowHR is a commercially provided Oracle/PeopleSoft Human Resources Management System (HRMS) that provides web-based management functions to allow USDA and its customers to access Federal employee, applicant, and contractor information from a centralized database maintained by their human resources and/or contracting departments.

System functionality includes recruitment, position classification, human resource (HR) processing, strategic workforce reporting, training and employee development, employee and labor relations, employee benefits administration, succession planning, employee performance, accountability, and organizational management. Employees can view their own personal information, and supervisors can review useful information about their employees.

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?

EmpowHR collects uses and maintains Federal employee, applicant, contractor and affiliate information that includes personally identifiable information (PII) including social security numbers (SSN), names, addresses, dates of birth, phone numbers, email addresses, and banking information.

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

Applicants, employees, contractors, managers and agency human resources offices provide information for EmpowHR.

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

EmpowHR serves as a repository to store job applications, personnel, and payroll data for the purpose of performing HR operations and administration of employee and contractor records.

1.4 How is the information collected?

Information is collected via a web-based application directly from employees, applicants, contractors and affiliates. HR staff may also enter information on an individual's behalf through the web-based application.

1.5 How will the information be checked for accuracy?

The HR Representative are responsible for the accuracy and completeness of any personal data provided. The HR Representative will be able to access, review, and update or correct their PII, unless access is prohibited by law or regulation. The HR representative validates the accuracy of PII before entering it into EmpowHR.

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

The Privacy Act of 197, as amended, 5 U.S.C. Sec. 552a governs the collection, use and safeguarding of data collected on individuals. Chief Financial Officers Act of 1990 Pub. L. 101-576

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

NFC complies with the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA), to ensure that data is protected from unauthorized access, malicious or inadvertent modification, disclosure, and disruption.

A Risk Assessment was performed on EmpowHR and security controls have been documented in the System Security Plan. These controls are tested annually under the continuous monitoring, SSAE 18, and A-123 programs.



Privacy Impact Assessment

NFC also works diligently to secure PII by requiring security awareness and privacy training to employees and contractors that have access to the data.

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.

Employee information is used to process personnel actions such as: hiring, separating, promoting, training, disciplinary issues, awards, work status, employee locator, performance evaluation, pay and leave calculation, health benefits, retirement, etc. The information collected is also used to assist applicants and potential applicants with the process of seeking employment with the Federal government. Contractor information is used to identify and manage non-employee personnel within an organization.

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

EmpowHR has data validation routines built into the interface which check for required fields, data types, and data ranges. Additionally, the business logic layer processes data before it is committed to the database, checking the data against business logic for accuracy and consistency.

Customer agencies may run pre-prepared and custom reports against the database and have the ability to access appropriate data elements depending on role and role-based security that has been granted.

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

The 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.

EmpowHR uses role-based access controls and Multi-Factor Authentication to protect access to all information. Employees only have access to their own records; managers have access only to employees they supervise; and agency human resources staff have access only to their agency employee information (as determined by the agency). Access to information is provided to individuals on a need-to-know basis and follows our "least privilege" policy. PeopleSoft, through PeopleTools, is used to manage end user security through role-based access controls.

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?

The retention period for contained in this system is covered by NARA General Records Schedules. NFC retains information in EmpowHR in accordance with NFC Record Schedule N1-106-10-7, which states a retention period of 56 years.

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

Yes. NFC Record Schedule N1-106-10-7 has been approved.

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

There is a risk that data may be retained longer than necessary. e. This risk is mitigated as NFC retains information in EmpowHR in accordance with NFC Record Schedule N1-106-10-7, which states a retention period of 56 years. Further, NFC removes data from online systems when appropriate and stores it offline at a federal records center or other authorized location, for the minimum amount of time required. NFC deploys masking and encrypts data at rest, and limits access based on the principle of least privilege. NFC also destroys data on paper and microfiche following the guidance and timelines in accordance with the NFC Record Schedule N1-106-10-7.

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?

Information collected by the EmpowHR system is owned by each customer agency. The customer agency determines the use and sharing of the information. NFC maintains and secures the information on behalf of NFC customers. The system/Agency Security Officers (ASO) handle all requests for any information pertaining to user accounts/access based on supervisory requests. Access is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties/access their data. Access is requested/determined by personnel/payroll offices who submit the data. NFC grants authority to use/access EmpowHR to individual users at the request of the agencies and approved by the user's ASO.

NFC provides agencies their own HR data from EmpowHR to (at their request), or to a service provider on their behalf. The agencies use the information as they deem necessary. NFC sends the requested data through authorized secure transmission mechanisms. The agencies are responsible for protecting and securing the data once it reaches its destination. Currently, data is being transmitted to the following agencies:

- USDA Forest Service
- USDA National Resources Conservation Service
- USDA Office of the Chief Information Officer

NFC shares our customers' EmpowHR data with other NFC MAs (Major Applications), as described below.

- Payroll/Personnel System: EmpowHR provides human resource data for use by the NFC Payroll/Personnel System.
- GovTA/webTA: EmpowHR provides human resource data for use by GovTA/webTA.
- Insight: EmpowHR provides HR data for use by the NFC Insight application.
- Web Applications: EmpowHR provides data for use by Web Applications (Reporting Center).
- OCIO Identity, Credential, and Access Management (ICAM) Shared Services system: EmpowHR provides data to the OCIO ICAM Shared Services Application, which provides authentication services for EmpowHR users. Additionally, as new USDA ICAM Shared Services users are authorized in EmpowHR, their names and information are stored in a database specifically for OCIO's use in managing the ICAM Shared Services Application Enterprise Entitlements Management Service (EEMS). EmpowHR also interfaces with ICAM Shared Services for identification and authentication services.

4.2 How is the information transmitted or disclosed?

The NFC EmpowHR data is transmitted over secure connection to internal and external connections. NFC discloses EmpowHR based on the routine uses based in the SORN, USDA/OP-1, Personnel and Payroll System for USDA Employees – 63 FR 4213 (January 28, 1998). Information is shared with other USDA systems as described in 4.1 above.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The system security officer handles all requests for and information pertaining to user accounts. Access control is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties. Access is requested/determined by personnel/payroll security officers (designated representatives) for offices who submit the data. NFC will grant authority to use/access EmpowHR to individual users at the



Privacy Impact Assessment

request of OPM and the requesting user's agency security officer. Data transmission risks are mitigated by the required use of secure file transmission methods for all information that is exchanged between EmpowHR and another system, agency, or organization.

Risk when sharing within USDA is considered low to moderate. Should data sharing include sources outside? of the network, encryption protocols ensure PII is not shared in an unencrypted format. Data is encrypted in motion and at rest. In addition, access to data is limited to only those persons with need-to-know through the use of an internal, granular governance process. Dissemination of information is governed by internal policy. Access to information is monitored, tracked, logged, and audited using tools such as Cloudera Navigator and Cloudera Manager.

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?

Information collected by the EmpowHR system is owned by each customer agency. The customer agency determines the use and sharing of the information. At their request, NFC provides some internal organizations (customer agencies) or their designated service providers with their data, as listed below, via secure transmission methods.

The agencies use the information as they deem necessary, and they are responsible for protecting and securing the data once it reaches its destination.

- Onboarding for OneUSDA: EmpowHR exchanges data with Onboarding (third party applications) hosted at the Department of Commerce (DOC) data center located in Alexandria, VA.
- USA Staffing: EmpowHR exchanges HR data with USA Staffing (USAS), a third-party application, hosted at the Office of Personnel Management (OPM) data center in Macon, GA.
- Monster Hiring Management Enterprise (Monster Government Services): EmpowHR exchanges HR data belonging to AOC employees with Monster Government Services (MGS) Monster Hiring Management Enterprise (MHME), a third-party application, hosted at the Equinix data center in Ashburn, VA.
- GDCI General Support Systems: EmpowHR provides HR data to GDCI GSS for use by GDCI GSS applications used by USDA. For example, EmpowHR sends user profile data (PII) to the "Onboarding Portal" provided by the ConnectHR application. EmpowHR also provides FS HR data for use in FS' Time and Attendance processing system (Paycheck8). EmpowHR provides Forest Service' (FS) HR data from EmpowHR to GDCI GSS at Forest Service's request, for use in the GDCI GSS Human Resource Management/Customer Relationship Management (HRM/CRM) application used by Forest Service.
- FEMA Operational Data Store/Enterprise Data Warehouse: EmpowHR provides FEMA HR data to the FEMA Operational Data Store/Enterprise Data Warehouse System.

- Library of Congress (LOC): EmpowHR provides LOC HR data to LOC for further processing.

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.

Yes, the sharing of PII outside the Department is compatible with the original collection, and is covered by USDA/OP-1, Personnel and Payroll System for USDA Employees – 63 FR 4213 (January 28, 1998), available on the USDA SORN website, <https://www.usda.gov/home/privacy-policy/system-records-notices>. The full OP-1 SORN is available from the following link: <https://www.govinfo.gov/content/pkg/PAI-2023-USDA-interim/xml/PAI-2023-USDA-interim.xml#op1>.

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

Information is accessed by customer agencies via a Web-based application which uses 128-bit encryption HTTPS. Disclosure of information is restricted through the use of multi-factor authentication (MFA) and sign-on protocols. Data is restricted through a profiled access approach. Only individuals with an established “need-to-know” may access their specific profiled data.

Any information transmitted from EmpowHR to an external agency (or their designated provider) must be transmitted via secure transmission, such as SFTP, over a Virtual Private Network (VPN) or other secure transmission protocols, as described in 5.1 above

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

Only authorized individuals can access information under the “need-to-know” authorities. The proper controls are in place to protect the data and prevent unauthorized access. Data transmission risks are mitigated by the required use of secure file transmission methods for all information that is transmitted from EmpowHR to another agency or organization. Data transmission methods currently used by EmpowHR are described in 5.1 above.

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.

Yes, SORN: USDA/OP-1 Personnel and Payroll System for USDA Employees – 63 FR 4213 (January 28, 1998), available at: <https://www.govinfo.gov/content/pkg/PAI-2021-USDA/xml/PAI-2021-USDA.xml#op1>.

The agencies that employ individuals are responsible for obtaining authorization to collect use, maintain, and share PII. NFC provides the agencies with the System of Record Notice (SORN) that is associated with EmpowHR. The agencies that use EmpowHR are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The individual employees must coordinate directly with their employing agency regarding these rights. <https://usda.empowhr.gov>

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

NFC customers are responsible for providing notice to their employees prior to collection of PII.

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

The agencies that employ individuals are responsible for providing individuals with the opportunity and/or right to decline to provide information, and also the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII. The agencies that use EmpowHR are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in USDA/OP-1, Personnel and Payroll System for USDA Employees - 63 FR 4213 (January 28, 1998). . The individual employees must coordinate directly with their employing agency regarding these rights.

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

The agencies that use EmpowHR are responsible for making their employees aware of, and consent to, use of their information for legitimate uses described in USDA/OP-1, Personnel and Payroll System for USDA Employees - 63 FR 4213 (January 28, 1998). The agencies are responsible for informing their employees of their rights to consent to particular uses of their information, as described in the SORN. The individual employees must coordinate directly with their employing agency regarding these rights.

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

NFC coordinates and communicates with the agencies that employ individuals, not directly with the employees. The agencies that use EmpowHR are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in USDA/OP-1, Personnel and Payroll System for USDA Employees - 63 FR 4213 (January 28, 1998). SORN. The agencies are responsible for informing their employees of their rights to consent to particular uses of their information, as described in the SORN. The individual employees must coordinate directly with their employing agency regarding these rights.

From a regulatory and management controls perspective, a copy of the redacted PIA is available on USDA's Office of the Chief Information Officer website, <https://www.usda.gov/home/privacy-policy/privacy-impact-assessments>.

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?

At the customer agency's discretion, and according to the agency's security policies, individuals may be assigned a unique user id and MFA that allows them access to their own data in the system.

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

Individuals with the proper assigned user role are able to correct specific information about themselves; however, most information in the system must be corrected by authorized users from the agency's human resources department at the request of the individual or at agency direction.

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

Each agency using the system will provide this information to employees.

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

Individuals with the proper assigned user role are able to correct specific information about themselves; however, most information in the system must be corrected by authorized users from the agency's human resources department at the request of the individual or at agency direction.

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

It is the responsibility of each individual agency to ensure that personnel with access to correct data on employees have the proper clearances, position sensitivity designations, and appropriate system access to the data. NFC access control procedures, role-based security of the application, and agency reporting of employee access and utilization aid agency officials in mitigating the risks of improper access to employee data.

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?

There are USDA Departmental Regulations and Access Management Standard Operating Procedures that govern security access management business process.

8.2 Will Department contractors have access to the system?

Yes, if authorized, contractors have access to the system.

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

Privacy and PII training is included in the Security Awareness and Rules of Behavior training 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. Contractors must complete annual security and privacy training, as well as be properly trained on the system.

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

Yes, 12/31/2023

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

EmpowHR provides auditing at the application, database, and network/operating system levels.

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.

8.6 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?

A Risk Assessment was performed on EmpowHR and security controls have been documented in the System Security Plan. These controls are tested annually under the continuous monitoring, SSAE 18, and A-123 programs.

NFC also works diligently to secure PII by requiring adequate training to employees and contractors that have access to the data. All employees and contractors adhere to privacy and security requirements for handling and storing of Federal data as directed by the Electronic Government Act Title III, also known as the Federal Information security Management Act (FISMA). Only role-based access is granted.

Controls are in place to protect the data and prevent unauthorized access. Access controls are based on the principle of least privilege, which refers to granting the minimum required system resources to a user to enables them to perform their duties. Access is requested/determined by personnel/payroll agency security officers (designated representatives) for offices who submit the data. The Office of the Chief Information Officer/Information Security Center//Information Technology Service Center/Access Management Branch, access account managers will grant authority to use/access EmpowHR to individual users at the request of USDA and/or user's agency security officers. Employees have access only to their own records; managers have access only to employees they supervise; and agency human resources staff have access only to their agency employee information (as determined by the agency). PeopleSoft, through its PeopleTools, manages the end user security. PeopleSoft has role-based and role-based security controls in place.

Data is encrypted in motion and at rest. Risk when sharing within USDA is considered low to moderate. Should data sharing include sources outside of the USDA network, encryption protocols ensure PII is not shared in an unencrypted format.

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?

EmpowHR uses a Commercial off-the-shelf (COTS) application.

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

There are no privacy concerns with the technology employed. NFC performs a privacy impact assessment to ensure that privacy concerns are identified and mitigated.

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.

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

N/A.

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

EmpowHR receives PII data from eRecruit, Onboarding, USA Staffing, and Monster that includes SSN, name, address, date of birth, phone number, email address, performance rating, etc., of employees, as well as voluntary self-identification of race and national origin identification data and disability designation.

EmpowHR sends USDA PII data to GDCII for use in ConnectHR that includes SSN, name, address, date of birth, phone number, and email address.

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

NFC uses the PII data from eRecruit, Onboarding, USA Staffing, and Monster to populate EmpowHR with payroll and personnel data about the person who has been selected for a position for the purpose of performing HR operations and administration of employee and contractor records.

The information collected from eRecruit, Onboarding, USA Staffing, and Monster is used in EmpowHR to assist applicants and potential applicants with the process of seeking employment with the Federal government. Employee information is used to process personnel actions and assist employees with hiring, separating, promoting, training, disciplinary issues, awards, work status, employee locator, performance evaluation, pay and leave calculation, health benefits, retirement, etc. Contractor and affiliate information is used to administer non-employee personnel within an organization.

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?

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database and is maintained and secured as part of EmpowHR. EmpowHR uses role-based access to all information. Employees only have access to their own records. PeopleSoft, through its PeopleTools, manages the end user security.

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

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database and is maintained and secured as part of EmpowHR. The retention periods of data contained in this system are covered by NFC Record Schedule N1-106-10-7. Civilian Personnel Records have various retention periods for specific types of data. These retention periods are adhered to per customer agency requirements and memorandum of understanding.

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

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database and is maintained and secured as part of EmpowHR. EmpowHR uses role-based access to all information. Employees only have access to their own records. PeopleSoft, through its PeopleTools, manages the end user security.

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?

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database, and is maintained and secured as part of EmpowHR. HR data stored in EmpowHR is owned by each customer agency. The customer agency determines the use and sharing of the information. At their request, NFC provides some internal/external organizations (customer agencies) or their external designated service providers with their data, as listed above in 4.1 and 5.1, via secure transmission methods.

The agencies use the information as they deem necessary, and they are responsible for protecting and securing the data once it reaches its destination.

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)?

No; the data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database and is maintained and secured as part of EmpowHR. See USDA/OP-1, Personnel and Payroll System for USDA Employees Customer agency SORN as reference.

10.10 Does the system use web measurement and customization technology?

No.

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?

N/A.

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.

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database and is maintained and secured as part of EmpowHR.

The system security officer handles all requests for and information pertaining to user accounts. Access control is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties. Access is requested/determined by personnel/payroll offices who submit the data. NFC will grant authority to use/access EmpowHR to individual users at the request of OPM and the requesting user's agency security officer.

Agency Responsible Officials

TRUDY
SANDEFER

 Digitally signed by TRUDY
SANDEFER
Date: 2023.09.01 12:01:45 -05'00'

Trudy Sandefer,
Information System Owner
OCFO, NFC
United States Department of Agriculture

Agency Approval Signature

TRACY HASKINS

 Digitally signed by TRACY HASKINS
Date: 2023.09.05 14:35:30 -04'00'

Tracy Haskins,
Information System Security Manager
OCIO, DAITO
United States Department of Agriculture