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	GovTA Application
Program Office	Government Employees Services Division (GESD)
Mission Area	OCFO, National Finance Center
CSAM Number	2609
Date Submitted for Review	02/07/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Nija Enclarde	Nija.enclarde@usda.gov	318-955-1393
Information System Security Manager	Tracy Haskins	Tracy.Haskins@usda.gov	202-720-8245
System/Program Managers	Trudy Sandefer	Trudy.Sandefer@usda.gov	504-426-1178

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 National Finance Center (NFC) is a Shared Service Center (SSC) under the Office of Personnel Management (OPM) Human Resources Line of Business (HRLOB). To carry out its wide-ranging responsibilities, the U.S. Department of Agriculture (USDA), and its employees and managers have access to diverse and complex automated information systems, which include system, file servers, local and wide area networks running various platforms, and telecommunications systems to include communication equipment.

The USDA relies on its information technology systems, including the Time and Attendance application (GovTA) to accomplish its mission of providing cost-effective and reliable services to the USDA and other serviced Federal agencies.

The NFC Government Employees Services Division (GESD), which falls under the United States Department of Agriculture (USDA), is responsible for development, deployment, maintenance, and testing of the NFC GovTA major application (MA).

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).

The GovTA system consists of time and attendance payroll data needed to conform to all applicable laws, Government regulations and procedures, and the needs of the Department and agencies in carrying out their time and attendance management responsibilities.

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 NFC GovTA application (GovTA) is a commercial off-the-shelf (COTS) web-based time and attendance (T&A) application specially designed and developed by the Ultimate Kronos Group (UKG) to meet the T&A reporting requirements for Federal Departments or Agencies and their employees. It is used by some NFC clients to manage government employee time and attendance functions.

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?

Chief Financial Officers Act of 1990 Public Law 101-576, authorizes the collection, the information maintained in this system

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

Yes

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

OCFO/NFC-01

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

Yes, the collection of information is covered by the Paperwork Reduction Act. The purpose and use of the data include recording, processing, and reporting the time and attendance data for USDA and other Federal agencies.

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

The application consists of name, encrypted Social Security numbers (SSN), time and attendance information included in teleworking agreements, and payroll data needed to conform to all applicable laws, Government regulations and procedures, and the needs of the Department and agencies in carrying out their personnel management responsibilities.

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

Federal agencies, employees, managers, agency human resources offices, and agency payroll/personnel offices provide information for GovTA.

2.2.1. How is the information collected?

Information is collected via a web-based application from Federal agencies, employees, and affiliates. Human Resource (HR) staff may enter information on an individual's behalf. Agencies may submit and receive data via Connect Direct and secure File Transfer Protocol (FTP) over a VPN connection. Only individuals with an established "need-to-know" may access their specific profiled data.

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

Not applicable

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

Employees, supervisors, and authorized users from the agency's payroll/personnel human resource departments are responsible for the accuracy and completeness of time and attendance data provided. Additionally, Payroll Personnel System (PPS) application code conducts routine reconciliation at the application level. These are maintained on the mainframe and applied to data entered and data transferred. As time and attendance documents are processed each pay period, data is processed through extensive error-checking routines.

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

Not applicable

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

Not applicable

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

No PII is captured through the use of 3rd party websites and/or 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.

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 purpose and routine use of the data include recording, processing, and reporting the time and attendance data for USDA and other Federal agencies.

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.

GovTA has data validation routines built into the interface that checks 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. Individuals and agencies may run predefined and custom reports against the data and can access data elements depending on access privileges requested by authorized agency personnel.

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?

Notice is provided to individuals prior to collection digitally at webTA| Login as well as via the SORN USDA/NFC-01

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

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. NFC provides the agencies with the SORN that is associated with GovTA. The agencies that use GovTA 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.

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 the following mitigation actions can better protect individual privacy rights and comply with privacy act requirements:**

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.

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

Accessibility: Make privacy notices easily accessible on websites and apps, ensuring they can be found without difficulty.

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?

Records are retained and disposed of in accordance with approved NARA guidance, NFC Records Control Schedule N1-016-10-7. Pursuant to this records schedule, records 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. Record Control Scheduled N1-016-10-7 has been 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 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?

Information collected by GovTA 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 our customers. The system/agency security officers 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 GovTA to individual users at the request of the agencies approved by the user's Agency Security Office (ASO).

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

1. NFC PPS System: GovTA uses human resources data provided by USDA and non-USDA Federal Employees, former employees, contractors, permittees, cooperators, and applicants for Federal employment whose personnel, payroll, and time & attendance records are serviced by NFC are covered by the system.
2. CIO authentication (eAuth) application: The eAuthentication application provides authentication services for some GovTA customers.
3. TIME: GovTA transmits certified T&A data to the PPS TIME application.

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.

Regular Training: Provide ongoing training for employees on data privacy policies, the importance of protecting PII, and how to handle it securely.

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?

Information is collected via data entry and front-end interfaces from individuals, customers, and agencies. Agencies submit data via Connect Dire and file transfers that use Secure File Transfer protocol (FTP) over Virtual Privacy Network (VPN) connection. The GovTA application uses 128-bit encryption HTTPS.

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?

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

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

Information in the system must be corrected by authorized users from the agency's payroll/personnel human resources department at the request of the individual or at agency direction. Procedures for correcting inaccurate or erroneous information is outlined in 2024-01680 OCFO NFC1 SORN.pdf

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

The SORN USDA/NFC-01 provides individuals seeking to contest or amend information maintained in the system procedures on correcting their information. The SORN can be located at: 2024-01680 OCFO NFC1 SORN.pdf.

Individuals seeking to gain access to a record in this system of records may contact the NFC Director at the address listed below. Provide the NFC Director with the necessary particulars such as full legal name, date of birth, work address, country of citizenship. Requesters must also reasonably specify the record contents sought. The request must meet the requirements of the regulations at 34 CFR 5b.5, including proof of identity. All requests for access to records must be in writing and should be submitted to the NFC Director

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

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

Formal redress is provided. Procedures for redress are outlined in 2024-01680 OCFO NFC1 SORN.pdf

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.

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?

GovTA provides auditing at the application, database, and network/operating system levels. DISC handles and retain the information in accordance with DISC Manual SEC-0035-MP-002, Protection, Control, and Disposal of Documents, Media, and Other Sensitive Materials.

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

Role-base access control is employed to provide access to the information system.

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 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. 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.

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 Information Security Awareness and Rules of Behavior training that is required for all federal employees and contractors annually.