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	USDA-Archibus
Program Office	Office of Operations
Mission Area	Departmental Administration Information Technology Office
CSAM Number	2594
Date Submitted for Review	5/1/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Corey Medina	Corey.medina@usda.gov	202-573-2810
Information System Security Manager	Lisa McFerson	Lisa.mcferson@usda.gov	202-720-8599
System/Program Managers	Tariq Khalil	Tariq.khalil@usda.gov	202-381-6931

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 USDA-Archibus System leverages a Commercial Off-The Shelf (COTS) application hosted internally at Digital Infrastructure Services Center (DISC). Archibus is an integrated workplace management system (IWMS) that leverages applications to help support the agencies’ infrastructure and resources. Archibus contains applications (modules) that support space management, asset management, reservations management, work order management and parking management. The PIA is necessary because the Archibus system collects personally identifiable 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.

Archibus is a customizable (COTS) product that supports the Office of Operations (OO).

Archibus supports core business processes to support the management of USDA office space and facilities for USDA’s Office of Operations (OO), Food and Nutrition Service (FNS), Digital Infrastructure Services Center (DISC) and Rural Development (RD); by providing a tool that manages workflow tracking and reporting in the following areas:

- Office space Hoteling
- Conference Room Management
- Parking
- Corrective Building Maintenance
- Preventative Building Maintenance
- Work Orders
- Space Management
- Asset Management

Archibus is an Integrated Workplace Management System (IWMS) to help organizations manage staff office space and facilities. Archibus is made up of various applications from Space Management to Energy Consumption to help organizations manage their portfolios and realize cost savings.

OO has provided Archibus implementation/deployment, user training of implemented applications, and preparation of technical documents including user and administration manuals/guides.

Typical Transactions:

- By using Archibus all USDA employees can submit work order tickets that get routed to OO Facility Management Division (FMD) for approval and action.

- By using Archibus all USDA employees can submit reservations requests that get routed to the appropriate approval authority dependent upon the individual room configuration and availability.

Information Sharing:

The system gets a nightly feed from Identity Credential and Access Management (ICAM) program that provides employee information which is used to identify the division and building assignment for individuals as well as provide the ability to use Single Sign On (SSO).

Module Description:

Archibus includes seven modules that users can access in order to submit a request/ticket, these include:

- Reservations – to allow users to reserve conference rooms through the application or directly through Outlook, this helps with conference room efficient utilization.

- Hoteling – to allow users to reserve workstations or collaboration areas.

- Corrective Building Maintenance – to allow for work order management and tracking.

- Preventive Building Maintenance – to schedule maintenance of facility equipment, such as HVACs.

- Parking Management – to help USDA manage their parking resources.

- Space Management – to help USDA manage their space inventory and occupancy and track utilization of space.

- Asset Management – used by FNS and RD to track all of their government furnished equipment.

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?

Government Paperwork Elimination Act (GPEA, Pub. L. 105–277) of 1998; Freedom to E-File Act (Pub. L. 106–222) of 2000; Electronic Signatures in Global and National Commerce Act (E–SIGN, Pub. L. 106–229) of 2000; eGovernment Act of 2002 (H.R. 2458/Pub. L. 107– 347); GRAMM-LEACH-BLILEY ACT (Pub L. 106–102).

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?

USDA/OCIO-2 eAuthentication Service

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?

There is an Active Directory feed that includes employee name and USDA email which is used for SSO. In the Parking application, employees can submit their own information to fulfill the requirements for issuance of a parking permit which includes name, zip code, business email address, business phone number, and license plate information.

2.2.1. How is the information collected?

User input and ICAM.

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

No.

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

Active Directory serves as the main database for employee details used for user authentication. The Archibus app enforces strict relationships between tables and checks most information fields with multiple choice options to maintain the integrity and accuracy of the stored data.

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?

NA

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

None.

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 Archibus Parking module collects Name, business mobile number, business email, home zip code and personal vehicle license plate information from USDA employees requesting USDA parking permits at the South and Whitten Building complex. This information is used to issue physical parking permits and is shared with security in the event of an emergency. USDA employees have the option to manage the data collected.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No.

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

Follow the format below:

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

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

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

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

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

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

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

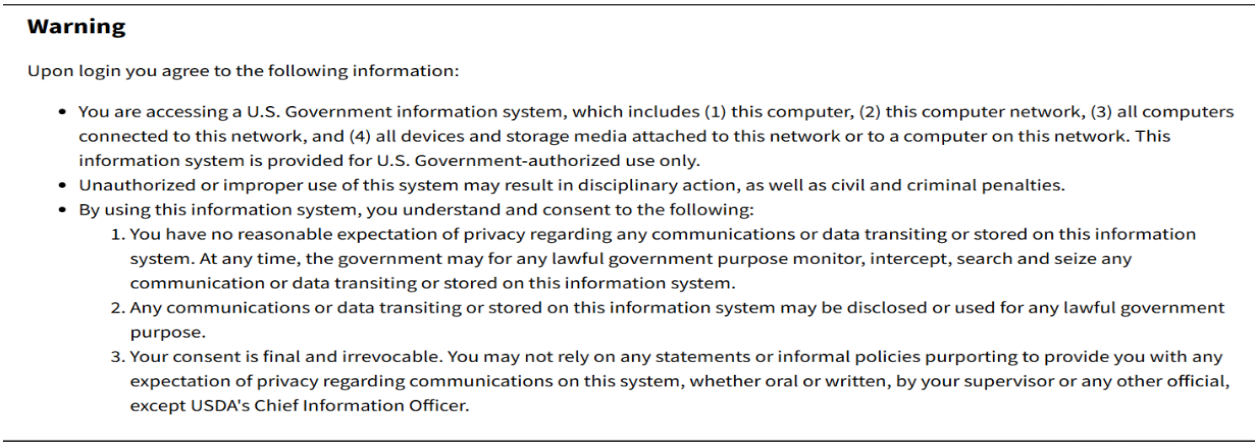
User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

This system is only accessible to the USDA employees and contractors with PIV (ICAM) multi-factor authentication (MFA) controls. Upon accessing the Archibus system, users are presented with the warning banner from ICAM as standard security and privacy practices. Please see the screenshot of the warning banner below. User information is derived from ICAM. Vehicle information is provided voluntarily as a prerequisite to obtaining a parking permit and users manage their own profile as it pertains to vehicle data.



Warning

Upon login you agree to the following information:

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  1. You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.
  2. Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.
  3. Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except USDA's Chief Information Officer.

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

Use of the system is completely voluntary. USDA employees and contractors use the Archibus system to submit building maintenance tickets, request parking permits, request conference room or hoteling space for action or approval.

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

Follow the format below:

Privacy Risk: Privacy Act risks associated with notices include:

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

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

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

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

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

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

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

Section 5: Data Retention

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

5.1. What information is retained and for how long?

The retention of data in the system is in accordance with applicable USDA records disposition schedules as approved by the National Archives and Records Administration (NARA). Records are maintained for varying periods, and temporary records are disposed of by shredding when the retention period is complete. Electronic records are sent to NARA, per the disposition document, after a period of five years. Records are maintained as an electronic copy in the system as needed for reference. The records schedule N1-016-08-3 outlines the following disposition schedule:

General Records Schedules:

5.4, Item 010 - Facility, space, vehicle, equipment, stock, and supply administrative and operational records.
Disposition Authority: DAA-GRS-2016-0011-0001
Temporary. Destroy when 3 years old or 3 years after
superseded, as appropriate, but longer retention is authorized if required for business use.

5.4, Item 070 - Facility, space, and equipment inspection, maintenance, and service records. (Structure and Long Term Maintenance)
Disposition Authority: DAA-GRS-2016-0011-0008
Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use.
OO Records related to Archibus system and its function of providing the ticketing:

3.1, Item 020 - Information technology operations and maintenance records.
Disposition Authority: DAA-GRS2013-0005-0004
Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

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. N1-016-08-3

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.

Obsolescence of Data: Retained data may become outdated or irrelevant, leading to inaccuracies in decision-making or service delivery, which can affect individuals negatively.

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

Data Retention Policy: Use NARA data retention policies that 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 system is not externally shared. ICAM provides user data for the purpose of authentication and SSO.

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

Follow the format below:

Privacy Risk: Sharing PII without following legal and regulatory requirements can lead to penalties.

Mitigation: 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?

The system is not externally shared/received/transmitted.

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

Follow the format below:

Privacy Risk: The system is not externally shared/received/transmitted

Mitigation: The system is not externally shared/received/transmitted

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?

Individuals who want to: know whether this system of records contains information about them, access their records, or contest the contents of a record, should make a written request to the Director, Office of the Executive Secretariat, U.S. Department of Agriculture, 1400 Independence Avenue SW., Washington, DC 20250. Individuals must furnish the following information for their records to be located and identified:

A. Full name or other identifying information necessary or helpful in locating the record.

B. Why does he or she believe the system may contain their personal information.
C. A statement indicating the type of request being made (i.e., access, correction, or amendment) and whether a personal inspection of the records or a copy of them by mail is desired.
D. Signature.

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

User data is transmitted electronically from ICAM on a nightly basis. If there are inaccuracies in a user's information (i.e. work email address, etc., workplace address, etc.), it is the user's responsibility to correct that information using the System Authorization Access Request (SAAR) process. Employees may correct erroneous information by updating their vehicle information directly in the system.

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

This PIA provided redress procedures at 7.1 above.

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

Redress procedures are provided.

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

Follow the format below:

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

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

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

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

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

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

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

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

Section 8: Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

8.1. How is the information in the system/project/program secured?

Archibus 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 encryption, to prevent misuse of data. 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 enable them to perform their duties.

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

Any authorized user which has access to the USDA network can utilize the system for building service requests, problem reporting, reservations, etc. Access to management functions within the system are role-based and access is granted based on job function.

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

The system gets a nightly feed from Identity Credential and Access Management (ICAM) program that provides employee information which is used to identify the division and building assignment for individuals as well as provide the ability to use Single Sign On (SSO).

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

USDA Information Security Awareness Training & Acknowledgment of Rules of Behavior are required by all federal employees and contractors. 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.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: Select a date.

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

Signed:_____

Signature of Responsible Officials

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

Signed:_____

<Name>
<System Owner>
<Agency>
U.S. Department of Agriculture

Signed:_____

<Name>
<Mission Area Privacy Officer>
<Agency>
U.S. Department of Agriculture

Signed: TRACY HENDRIX Digitally signed by TRACY HENDRIX Date: 2025.06.25 23:10:30 -04'00'

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