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..... 3

Mission Area System/Program Contacts..... 3

Abstract..... 4

Overview..... 4

Section 1: Authorities and Other Requirements 6

Section 2: Characterization of the Information 7

Section 3: Uses of the Information..... 12

Section 4: Notice 14

Section 5: Data Retention..... 16

Section 6: Information Sharing 18

Section 7: Redress 20

Section 8: Auditing and Accountability 22

Privacy Impact Assessment Review 23

Signature of Responsible Officials..... 23

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Conservation Delivery Streamlining Initiative (CDSI_NITC)
Program Office	Conservation Planning and Program Delivery
Mission Area	Natural Resources Conservation Service
CSAM Number	2086
Date Submitted for Review	

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Samantha Jones	Samantha.Jones@usda.gov	(202) 221-9928
Information System Security Manager	Lanita Thomas	Lanita.Thomas@usda.gov	202-260-8593
System/Program Managers	Krystal Casey	Krystal.Casey@usda.gov	000-000-000

Abstract

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

CDSI_NITC supports USDA’s Conservation Desktop Programs. The programs allow clients to request assistance with conservation problems, collaborate with the Natural Resources Conservation Service (NRCS) during financial planning processes, integrate with NRCS existing financial assistance programs and contract management. CDSI_NITC uses the information collected to help the NRCS field staff and NRCS customers in delivering conservation services efficiently. The PIA is being conducted because this system contains 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.

CDSI_NITC is owned by USDA’s Conservation Desktop Program within NRCS. The business purpose of the information technology system is to support NRCS customers with various conservation services. This relates to FPAC/FBC mission to support the passage of the Farm Bill, to strengthen financial systems accountability, to support the revision of NRCS’ strategic plan, support the need to more clearly define NRCS’ assistance for emerging issues, such as energy, air quality, greenhouse gases, and market-based initiatives, the growing need for nimble business processes that can rapidly respond to program changes, and the need for increase transparency and accountability for outcomes from NRCS conservation assistance.

It is estimated that approximately 25,000 NRCS farmers, ranchers, landowners, and Farmers.gov producers currently have information stored with CDSI_NITC. The user population will continue to grow as the need to support these user groups of various conservation services. CDSI_NITC is comprised of 8 applications, which include (1) Conservation Assessment Ranking Tool, (2) Conservation Desktop Financial Assistance, (3) Conservation Desktop Technical Assistance, (4) CDSI – Easement/Highly Erodible Land Conservation (HELC)/Wetland Conservation, (5) Conservation Partners Information Interchange, (6) Feature Flag Service-User Interface, (7) Guardian, (8) Limited English Proficiency Letter, and (9) Exhibit Generator. These applications allow clients to request assistance with conservation problems, collaborate with NRCS during financial planning processes, integrate with NRCS existing financial assistance programs and contract management, manage, and track highly erodible land conservation, support translation documents for different language users, and provide external facing services with conservation partners. This system only operates in the confines in NRCS conservation programs.

The legal authorities to operate the IT system include the following:

The legal authority to operate the IT system the Agriculture Improvement Act of 2018, Pub. L. No. 115-334 and the Inflation Reduction Act, Pub. L. 117-169.

The completion of this PIA will not result in changes to business processes or technology changes.

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 Agriculture Improvement Act of 2018, Pub. L. No. 115-334
- The Inflation Reduction Act, Pub. L. 117-169

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

Security Plan Status:	New plan in progress.
Security Plan Status Date:	August 30, 2024
Authorization Status:	Authorized to Operate
Authorization Status Date:	July 24, 2023
Authorization Termination Date:	July 24, 2026
Risk Review Completion Date:	June 20, 2024
FTPS 199 Classification of the System:	Moderate

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

USDA/NRCS, Landowner, Operator, Producer, Cooperator, or Participant Files[1].

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

No

[1] USDA System of Records Notices are found at https://www.govinfo.gov/content/pkg/FR-2005-08-30/pdf/05-17305.pdf

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?

CDSI collects information directly from the affected members of the public (i.e., landowners).

2.2.1. How is the information collected?

Information is collected from the public, which is transcribed from paper application forms.

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

This system does not use information from commercial sources or publicly available data.

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

Information in CDSI is reviewed for accuracy and is verified through manual review and comparison with existing agency data throughout the approval process upon data entry.

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

Yes

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

The separately accredited 3rd party eSignLive is used to allow clients to submit signed documents to CDSI components.

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

The document signers name, signature, and other applicable application data is collected and stored.

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?

This information collected is used to identify farmers, ranchers, landowners, and other customers of NRCS interacting with conservation planners and other specialists at the NRCS. Data collected by the CDSI application will be used to respond to requests for assistance with applicant's conservation problems, communicate/collaborate with NRCS during the planning and financial assistance processes, support the various steps of the conservation planning process; and to integrate NRCS' existing financial assistance programs contract management.

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.

The system uses open-source visualization, to support time-series analysis, log analysis, and monitoring of the system.

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?

Privacy Act Statements are placed on each form that collects PII. The statement notifies the individual of the authority to collect the information, what organizations may be legally authorized to receive it, how the information may be used, and individual's option to refuse to provide the information to USDA.

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

Individuals may decline to provide any of the information without penalty. However, refusing to provide some information could delay processing or result in the denial of their application. Users have the right to provide consent to access their information. To do so, the individual must make a written request to the information owner, system owner, or Privacy Officer to evaluate their request.

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?

All records found in CDSI_NITC are retained for 10 years and deleted only after the information is no longer needed for administrative, legal, audit or other operational purposes.

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.

The retention schedule has been approved by the USDA records office and NARA. The Records Schedule Number is NI-114-083[2].

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.

[2] https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-agriculture/rg-0114/n1-114-08-003_sf115.pdf

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?

This system does not share, receive, or transmit information internally.

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

Follow the format below:

Privacy Risk: Unauthorized access to sensitive data could pose a risk to existing data and disclosure to unauthorized parties.

Mitigation: Information is electronic transmission of the data is encrypted, and access is only granted based on a user's role and active/inactive status.

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?

This system does not share, receive, or transmit information externally.

6.4. **Privacy Impact Analysis**: Related to external 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.

Data Misuse: PII can be misused for purposes other than intended, leading to privacy violations.

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.

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?

Should an individual wish to gain access to their information, they will need to make a written request to the system owner or FPAC FOIA Officer, to authenticate their identity and identity the records they request access to.

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

Individuals must make a written request to the system owner, information system owner or Privacy Officer, authenticate their identity, identify the portion(s) of the record that needs to be corrected and describe who their information is inaccurate or erroneous. Upon receipt and review of the request, if it is verified a correction needs to be made, the record will be corrected and a sample of the document with the correction will be transmitted to the individual who made the request.

Requests to correct a record should be sent directly a local or state FSA Office. All requests (1) must be in writing, (2) clearly identify the information that needs correction, (3) provide a reason why the information is incorrect, and (4) state what the correction should be.

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

In addition to normal notification through the SORN process, field technicians provide correction procedures to individuals upon request.

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

Individuals may contact their administrative point of contact to obtain access to their information; or

Any individual may obtain information as to the procedures for contesting a record in the system which pertains to him/her by submitting a written request to the district conservationist or his/her designated representative or to the Director, Management Services Division, USDA Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013.

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

Follow the format below:

Privacy Risk: Privacy Act risks associated with redress include:

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

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

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

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

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

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

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

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

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?

CDSI_NITC applications are protected by encryption Federal Information Processing Standard 140-2 (FIPS-140-2),[3] masking of PII data, controlled access, timeout for remote access and audit logging. Access to the system is role-based and require multi-factor authentication for all accounts.

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

Access to PII is determined by user role and restricted access. Access to PII is granted by appropriate legal authorities. Applicable user and roles are documented in the System Security Plan.

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

Any time organizations outside of USDA requests access to information, a data sharing agreement is created and routed through the Grants and Agreements Office for review. The Grants and Agreements Office ensures all stakeholders, to include, but not limited to the FPAC Privacy Officer, a Senior Agency Official, and receiving organization official, review and sign the data sharing agreement that lays forth the standards and rules for handling USDA PII.

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

Annual organizational training, including USDA Information Security Awareness Training & Acknowledgment of Rules of Behavior, is mandatory for all federal and contractor staff working with CDST_NITC.