U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

Farm Program Business Partner & Farm Records System (MIDAS)

Program Delivery Division

Farm Service Agency

Date PIA submitted for review:

Mission Area System/Program Contacts:

	Name	**E-mail**	**Phone Number**
Mission Area Acting Assistant Privacy Officer	Samantha Jones	Samantha.Jones@usda.gov	202-221-9286
Information System Security Manager	Brian Davies	Brian.Davies@usda.gov	202-720-2419
System/Program Managers	Suman Sarekukka	Suman.Sarekukka@usda.gov	816-823-2949

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 Farm Program Business Partner & Farm Records System (MIDAS) supports various United States Department of Agriculture (USDA) Farm Service Agency (FSA) programs. These programs provide funds for maintenance and incremental improvements. The MIDAS Project was established to modernize initiatives to provide a secure, long-term, web-based solution to simplify, integrate, and automate the delivery of Farm Programs across the United States. 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.

MIDAS CRM is owned by USDA's FSA Program Delivery Division. The business purpose of the information technology (IT) system is to capture producer and farm records data for farmers and ranchers in the US who have requested to participate in Farm Service Agency (FSA), National Resource Conservation System (NRCS), and other USDA agencies per program requirements. This relates to FSA's mission to serve farmers ranchers, and agricultural partners through the delivery of effective, efficient agricultural programs for all Americans. The system was created to modernize initiatives to provide a secure, long-term, web-based solution to simplify, integrate, and automate the delivery of Farm Programs across the United States to support various USDA programs.

This system contains an estimated 14 million records of individuals and entities, who voluntarily provided their customer data on an OMB approved form prior to, or during a program application process. . The majority of these individuals and entities have previously participated or are currently participating in USDA programs. This system consists of 4 applications which include:

- **Farm Records** – this application views, establishes, and maintains farm records data.
- **Business Partner** – this application accesses and maintains Business Partner data from a single system of record for all FSA customers.
- **Product Master** - this application captures crop information and provides a full crop catalog.
- **Organizational Structure –** this application centralizes CRM employee access and roles to associated counties and positions from source systems.

These applications are accessible via the MIDAS Portal and authorizations which are assigned using USDA eAuthentication and CRM Organizational Structure, which controls the user's create, edit and view capabilities and drive workflows for approvals. Together these capabilities form a common system for a significant portion of FSA's core farm and producer data. These systems integrate with USDA and FSA web-based systems, improve data integrity and security, and ease producer burden by allowing access to update customer and farm information at any County Office. Business Partner and Farm Records (including Historical data from 1999 to current program year) is the System of Record and Entry for customer records and farm data which is shared with other applications and agencies across USDA using shared services. These secure and modernized systems support farm program delivery and integrated business processes which are used every day in FSA's 2,124 FSA offices to manage approximately 14 million producers, 5 million farms, 8.1 million tracts, and 38 million fields. MIDAS does not operate on more than one site.

The legal authority to operate the IT System is Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397. This PIA will not result in circumstances that require changes to existing business processes or technology changes.

Section 1.0 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 following legal authority permits the collection of information for MIDAS: Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397.

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

Security Plan Status:	Completed.
Security Plan Status Date:	April 5, 2024
Authorization Status:	Completed.
Authorization Status Date:	April 25, 2022
Authorization Termination Date:	April 25, 2025
Risk Review Completion Date:	April 10, 2024
FIPS 199 Classification of the System:	Moderate

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

These following covers MIDAS: SORN USDA/FSA-2[1] and SORN USDA/FSA-14[2].

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

[1] sorn_fsa2_2019.pdf (usda.gov)

[2] sorn_fsa14_2019.pdf (usda.gov)

MIDAS information collection is covered by the Paperwork Reduction Act. Form AD-2047 is subject to this Act. Additionally, the Customer Data Worksheet Request for Business Partner Record Change OMB Control number 0560-0265 supports this collection.

Section 2.0 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	☐	License Plate Number
☐	Registration Number	☐	File/Case ID Number
☐	Student ID Number	☐	Federal Student Aid Number
☐	Passport number	☐	Alien Registration Number
☐	DOD ID Number	☐	DOD Benefits Number
☒	Employee Identification 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	☒	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number		

Biographical Information					
☒	Name (including nicknames)	☒	Gender	☒	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
☒	Citizenship	☒	Immigration Status (Resident Alien Status)	□	Religion/Religious Preference
☒	Home Address	☒	Zip Code	☒	Home Phone or Fax Number
☒	Spouse Information	□	Sexual Orientation	□	Children Information
☒	Marital Status	□	Military Service Information	□	Mother's Maiden Name
☒	Race	☒	Nationality	☒	Global Positioning System (GPS)/Location Data (geospatial farm/CLU boundaries)
☒	Personal e-mail address	☒	Business e-mail address	□	Personal Financial Information (including loan information)
□	Employment Information	□	Alias (username/screenname)	□	Business Financial Information (including loan information)
□	Education Information	□	Resume or curriculum vitae	□	Professional/personal references

Biometrics/Distinguishing Features/Characteristics

□	Fingerprints	□	Palm prints	□	Vascular scans
□	Retina/Iris Scans	□	Dental Profile	□	Scars, marks, tattoos
□	Hair Color	□	Eye Color	□	Height
□	Video recording	□	Photos	□	Voice/ Audio Recording
□	DNA Sample or Profile	□	Signatures	□	Weight

Medical/Emergency Information

□	Medical/Health Information	□	Mental Health Information	☒	Disability Information (if customer declared)
□	Workers' Compensation Information	□	Patient ID Number	□	Emergency Contact Information

Device Information

□	Device settings or preferences (e.g., security level, sharing options, ringtones)	□	Cell tower records (e.g., logs, user location, time, etc.)	□	Network communications data

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 (IRS-Validated Tax ID Number)

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

The information is supplied directly from customers declared on an OMB approved form and county offices entered the data into the system, and employee access and associated roles sourced from EAS, MRT, and EmpowHR. FSA Internal Sources also include Business File System (entity structure), Common Eligibility System (Subsidiary), , and Conservation Reserve Program (CRP-contract).External sources include Social Security Administration (SSA) (deathmaster file) and Internal Revenue Service (IRS) (TIN matching). .

2.2.1. How is the information collected? (2.2a)

MIDAS Release 1 included the Farm Records system of record for current year data entered through MIDAS Farm Records. Prior year Farm Records system of record data continued through the Farm Records System until FY 2023. Prior to MIDAS Release 2, customer information was manually entered [using the Service Center Information Management Services (SCIMS) system] at County Offices on at the request of producers seeking to participate in FSA programs. (Within Release 2, the system of record became MIDAS CRM BP rather than SCIMS.) Information is also shared from other FSA systems with which MIDAS has documented interconnections. In February 2023, all prior year farm records data from Web FRS was migrated to MIDAS Farm Records. MIDAS Farm Records is now the system or entry for all current and prior year farm records.

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

N/A

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

Data collected from the customer is required by policy to be review for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made. The participant can request changes to their customer data stored in the system using an OMB-approved form. FSA will initiate changes to a farm record based on producer provided information or when new official imagery is received that identifies changes to the land.

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

No

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

N/A. Farm Records GIS leverages outside services to display and identify the location of a farm. No PII is accessed for this purpose.

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

No. PII is made available using this third-party website. Services from outside sources are accessed to assist with identifying a location only.

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 3.0 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?

Producer and farm information is used to participate in USDA programs. No additional “tools” (other than the application and database itself) are used to analyze the data. System users do not add publicly available data. National agriculture Imagery Program (NAIP) imagery is used to establish and maintain the geospatial footprint of the delineated farm, tract, and field boundaries in Farm Records. NAIP is considered public domain.

The information is processed by the system as producers apply to participate in FSA and NRCS programs. Information is collected to establish eligibility and certification for payment of program benefits on commodities/crops or farmland.

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 4.0 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?

FSA Privacy Policy states that “Submitting information is strictly voluntary.”

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

Yes, in accordance with FSA Privacy policy and the individual's written consent.

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 5.0 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 current requirement is to maintain 20 years of historical data and archive records that are older. Retention of some data is for shorter periods and varies by data type and by Program.

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, the retention schedule is in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records.

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 6.0 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?

NRCS, RMA, and FSA agencies share/receive/transmit -Farm Record and Business Partner data for program delivery purposes. Data transmission is protected by encryption including Transport Layer Security (TLS) 1.2.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Information is shared internally between NRCS, RMA, FSA agencies is at risk for unauthorized access.

Mitigation: Information is transmitted via encrypted communication channel. Data is controlled by role-based access and only available to users with authorized access.

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?

Internal Revenue Service (IRS) TIN and name matching (batch files with Tax Identification Number (TIN) and legal name information) and the SSA (Death Master) are external organizations that share/receive/transmit this data.

Encryption is implemented for electronic files sent to outside organizations. Data transmission is protected by encryption including Transport Layer Security (TLS) 1.2.

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 7.0 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?

As published in SORN USDA/FSA-2 and SORN USDA/FSA-14: "An individual may obtain information about a record in the system which pertains to such individual by submitting a written request to the above listed System Manager. The envelope and letter should be marked ``Privacy Act Request.'' A request for information should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

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

As published in SORN USDA/FSA-2 and SORN USDA/FSA-14: "Individuals desiring to contest or amend information maintained in the system should direct their request to the above listed System Manager and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

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

Individuals are required to complete a new Customer Data Worksheet AD-2047 to correct their customer information.

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

Individuals can contact any USDA Service Center to request correction to their customer or farm information.

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?

Information in the system is secured by encryption with AES-128 or AES-256-bit encryption including Transport Layer Security (TLS) 1.2.

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

FSA-13-A is used to request user access to USDA and FSA information technology systems including specifying authorization for accessing the system. (Refer to Notice IRM-440) In addition, access to FSA web applications is gained via an on-line registration process like using the FSA-13-A form. Access to the application is supported by MFA for all users based on need to know. Data transfer and retention of information is secured by AES-128 or AES-256-bit encryption including Transport Layer Security (TLS) 1.2.

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

Data sharing requirements are met between USDA mission areas via interconnection agreements

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

Once hired, privacy training and security awareness training is completed prior to gaining access to a workstation. The privacy training addresses users’ responsibilities to protect privacy data and how to protect it.

Approval Signatures:

Doug Jones
System Owner
Farm Production and Conservation – Farm Business Center
United States Department of Agriculture

Samantha Jones
Mission Area Acting Assistant Privacy Officer
Farm Production and Conservation – Farm Business Center
United States Department of Agriculture

James Flickinger
Assistant Chief Information Security Officer
Farm Production and Conservation – Farm Business Center
United States Department of Agriculture

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.06.08 20:24:48 -04'00'

Office of the Chief Privacy Officer
United States Department of Agriculture