U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

Privacy Impact Assessment

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 Programs Price Support System (FPPSS)

Program Delivery Division

Farm Service Agency

Date PIA submitted for review:

December 22, 2023

Mission Area System/Program Contacts:

	Name	**E-mail**	**Phone Number**
Mission Area Privacy Officer	Deryl Richardson	Deryl.Richardson@USDA.gov	323-533-3020
Information System Security Manager	Jerry Hagedorn	Jerry.Hagedorn@USDA.gov	816-926-2141
System/Program Managers	Doug Jones	Doug.Jones@USDA.gov	816-926-2758

Abstract

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

The Farm Programs Price Support System (FPPSS) supports the United States Department of Agriculture's (USDA) Commodity Loan and Loan Deficiency Payment programs. The two programs assist producers upon harvest and shearing, aiding in the sale of commodity when favorable marketing conditions occur. FPPSS uses the information collected to process producer applications and service loan disbursements. 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. Noted..

FPPSS is owned by USDA's Commodity Loan and Loan Deficiency Payment programs within USDA's Farm Service Agency (FSA). The business purpose of the information technology (IT) system is to facilitate processing loans, which tie in with the program's mission to provide loan assistance to meet cash flow needs during harvest time. 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, which users include applicants and USDA FSA staff employees, was created to provide county and state offices with automatic software applications to support the administration of the Commodity Loan and Loan Deficiency Payment programs. The two programs assist producers upon harvest and shearing to aide in the sale of commodity when favorable marketing conditions occur.

It is estimated that approximately 49,000 individuals may currently have information stored within FPPSS. Because the farm programs supported by FPPSS are subject to varying levels of participation among agricultural producers based upon a variety of factors, including market prices for supported commodities, weather, and environmental conditions, as well as other circumstances which may impact the agricultural economy, the number of individuals who may be included in FPPSS will vary over time. Only the necessary information to disperse and receive payments is collected in the system. FPPSS is currently comprised of 11 applications, which include the (1) Automated Cotton Reporting System, (2) Commodity Loan Processing System, (3) Cooperative Marketing Association System, (4) Cotton On-Line Processing System, (5) Electronic Warehouse Receipts, (6) Electronic Loan Deficiency Payments, (7) Interim Market Gain/Loan Deficiency Payment Processing Application, (8) Loan Deficiency Payments, (9) Peanut Market Place and Data Collection, (10) ShadowBase, and (11) State Office Reporting System. The applications process applicants, disburse loans, make payments, perform servicing transactions, track and report on loans, loan deficiency payments, marketing assistance, and market loss program payments. The system is only operated within the confines of FSA staff offices.

The legal authority to operate the IT system is the Protection of Purchases of Farm Product, 7 U.S.C. 1631; Commodity Credit Corporation Act, 15 U.S.C. 714; the Agriculture Improvement Act of 2018, PL 115-334; and Cooperative Marking Associations, 7 CFR 1425. The PIA will not require or result in changes to existing business processes or technology.

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 System of Records Notice (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 Protection of Purchases of Farm Product, 7 U.S.C. 1631; Commodity Credit Corporation Act, 15 U.S.C. 714; the Agriculture Improvement Act of 2018, PL 115-334; and Cooperative Marking Associations, 7 CFR 1425.

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

Security Plan Status:	Completed. New Security Plan underway.
Security Plan Status Date:	June 2, 2022
Authorization Status:	Completed. New Authorization is underway.
Authorization Status Date:	May 17, 2022
Authorization Termination Date:	May 17, 2025
Risk Review Completion Date:	July 20, 2023
FIPS 199 Classification of the System:	Moderate

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

The following SORNs[1] cover FPPSS: Farm Records File USDA/FSA-2 and Applicant/Borrower USDA/FSA-14.

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.usda.gov/home/privacy-policy/system-records-notices.

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 Number

Check Box	Identifying Number	Check Box	Identifying Number
☒	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

Check Box	Biographical Information	Check Box	Biographical Information	Check Box	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	☐	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
☐	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

Privacy Impact Assessment

Biometrics/Distinguishing Features/Characteristics

Check Box	Biometrics/Distinguishing Features/Characteristics	Check Box	Biometrics/Distinguishing Features/Characteristics	Check Box	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

Check Box	Medical/Emergency Information	Check Box	Medical/Emergency Information	Check Box	Medical/Emergency Information
☐	Medical/Health Information	☐	Mental Health Information	☐	Disability Information
☐	Workers' Compensation Information	☐	Patient ID Number	☐	Emergency Contact Information

Device Information

Check Box	Device Information	Check Box	Device Information	Check Box	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

Check Box	Specific Information/File Types	Check Box	Specific Information/File Types	Check Box	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

Additional PII collected, but not listed above, include customer identification number, eAuthentication (eAuth)[2], marketing assistance loan number, commodity loan number, and loan deficiency payment number.

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

The information is supplied directly from program participants and authorized external entities such as cooperative marketing associations, loan service agents, electronic warehouse receipt providers, and peanut shellers. Information is also obtained from internal FSA databases such as the service center information management system.

2.2.1. How is the information collected?

Information is collected from the program participants of the programs.

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?

Program staff and participants check information upon data entry. Additionally, program staff review participant information when updates are made.

---

[2] USDA eAuth is the system used by USDA agencies to enable individual customers and employees to obtain accounts that will allow them to access USDA Web applications and services via the Internet.

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

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

N/A

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

Privacy Risk: *T*he information collected contains sensitive PII, which if disclosed, would cause an unwarranted invasion of personal privacy.

Mitigation: *T*he information is only disclosed to those responsible for the administration of the program or other entities that have legal authority to access the information. Users are required to authenticate their identity prior to accessing the information and access is restricted based upon user role.

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?

The information collected is used to support the Commodity Loan and Loan Deficiency Payment programs. Specially, the information is used to determine eligibility, process applicant information, disburse loans, make payments, service transactions, and generate reports.

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.

Privacy Risk: Access to the data collected must be monitored to ensure safeguarding against unauthorized access and use.

Mitigation: Access to PII is determined by the owner of the information, user roles, and restricted access. Additionally, access will only be granted to the PII upon appropriate legal authority.

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?

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

Privacy Risk: The information collected in accordance with USDA/FSA-2 and USDA/FSA-14 is part of a Privacy Act System of Records that requires safeguarding, access and disclosure when legal authority exists. The system information is specific to each individual and could cause moderate harm to the individual upon unauthorized disclosure.

Mitigation: As a result of the information being connected to SORNs, information in the system can be only accessed or disclosed upon legal authority or dictated routine use.

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?

All records found in FPPSS is 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 DAA-0145-2017-0018.

5.3. PRIVACY IMPACT ANALYSIS: **Related to retention of information.**

Privacy Risk: *T*he information contained in the records are sensitive, which could cause a privacy breach of not properly safeguarded.

Mitigation: *A*ccess and destruction of the information will only occur upon establishment of proper legal authority to access the data, pursuant the Privacy Act, Section 1619 of the Farm Bill, and the appropriate SORN(s) covering the information.

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?

None

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

Privacy Risk: N/A

Mitigation: N/A

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 shared with Electronic Warehouse Receipt (EWR Inc,) Peanut Shellers and the Federal State Inspection Service. Loan information, peanut quantities, grading details, and reconciliation of FSA-1007 [3]is the information shared to facilitate loan repayment. The information is transmitted over an encrypted communication channel.

---

[3] The FSA-1007 is a peanut "Inspection Certificate and Calculation Worksheet" form. The form contains inspection, grading and weight details for a load of peanuts delivered to a peanut buying point.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Privacy Risk: The sensitive information shared is at risk for unauthorized access.

Mitigation: Information is transmitted via encrypted communication channel. Data is controlled on provider system[4] using role-based security and is available only to individuals have the proper authorized access.

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?

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 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 the agency Privacy Officer or FOIA Office to obtain access to their information.

---

[4] A provider system is a database owned by EWR and is used to electronically file and maintain warehouse receipts and the United States Warehouse Act documents. EWR is a provider business which has an approved provider agreement in place with USDA Agricultural Marketing Service (AMS). AMS administers provisions of the United States Warehouse Act, including approval of EWR provider organizations.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Privacy Risk: The system information provided by participants is important to be accurate, as it has an impact on their program participation, as well as IRS reporting requirements. Incorrect information may adversely affect the participant or other individuals, result in denial of service or incorrect payments.

Mitigation: Individuals are provided with access to their information electronically to check for accuracy of their submission(s). Additionally, program staff will verify submitted information with the individual as well as previously collected data.

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?

The FPPSS employs a defense-in depth strategy. Web applications are protected by web application firewall and restrictive networking. The application server is configured using Center for Internet Security hardened images and all components employ end point protection and real-time monitoring for malicious activity. Access to the system is role-based and require multi-factor authentication for all accounts. All data transfer and storage utilize Federal Information Processing Standard (FIPS 140-2) compliant encryption.

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 the owner of the information, user roles, and restricted access. Additionally, access will only be granted to the PII upon a need to know. Applicable users and roles are documented in policy and procedure as well as system business rules, and 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 FPPSS.

Approval Signatures:

Signed copies kept on record.