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."

case

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	ePermits Legacy
Program Office	PPQ
Mission Area	MRP
CSAM Number	1206
Date Submitted for Review	

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Angela Cole	Angela.cole@usda.gov	202-465-6265
Information System Security Manager	Carl Remalia	Carl.remalia@usda.gov	240-428-9746
System/Program Managers	Vincent Selvidge	Vincent.selvidge@usda.gov	531-999-0463

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 primary objective of the USDA Animal and Plant Health Inspections Service (APHIS) ePermits Legacy system is to provide Plant Protection Quarantine (PPQ), Biotechnology Regulatory Services (BRS), and Veterinary Services (VS) with an ability to search and view historical permits and applications previously filed through the ePermits application. As the ePermits functionality has been replaced by the Salesforce-based 'eFile' application, the remaining 'ePermits Legacy' serves as a solution to access legacy data which was not migrated to eFile. This legacy system will require continued access by the APHIS team. ePermits Legacy contains the names, addresses, telephone numbers, email addresses and organization names of individuals who hold permits. It also contains the destination addresses for shipments of regulated articles, including the shipping contact names and phone numbers.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The ePermits Legacy Application is built using the secure and scalable Microsoft Power Platform. It allows USDA business users to retrieve APHIS legacy permit applications using various search criteria and present the results in a user-friendly format. Additionally, it provides an interface for business users to analyze data and respond to regulatory Freedom of Information Act (FOIA) requests. ePermits is no longer accepting new data and is read only. It has been replaced by e-File for new permits moving forward. The records in ePermits continue to be accessed as needed. Permits are shared with Customs and Border Protection (CBP). ePermits contain the information of around 70,000 individuals.

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 data stored in ePermits Legacy is authorized under USDA APHIS regulatory policy listed as follows:

- VS:
  - Animal Health Protection Act (7 U.S.C. 8301 et. seq.) 9 CFR Parts 93, 94, 95, 98, and 122
- BRS:
  - Plant Protection Act (7 U.S.C. 7701 et. seq.), 7 CFR Part 340: Movement of Certain Genetically Engineered Organisms; OMB 0579-0085 and 0579-0471
- PPQ:
  - Plant Protection Act (7 U.S.C. 7701 et. seq.) Parts 300 – end (incl. Endangered Species Act requirements)
  - Federal Seed Act (7 U.S.C. 1551-1611 as amended)
  - Honeybee Act (7 U.S.C. 281)
  - Agriculture Bioterrorism Act (7 U.S.C. 8401)

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

Yes. The existing ePermits Legacy application is classified as a Moderate system. It received an ATO on 4/25/2022 and expires on 9/25/2025. The System Security Plan (SSP) was signed on 8/22/2022. The last risk review was completed on 9/5/2025.

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

APHIS 10 SORN ([APHIS Comprehensive Electronic Permitting System (ePermits)](#)

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

At this present time, no new PII is collected as this is an archival system that is read only. Prior to this system becoming an archival system, it was covered by the Paperwork Reduction Act and the OMB numbers for the forms utilized are listed below:

VS:
0579-0015 – VS Form 16-3
0579-0040 – VS Forms 16-3, 17-129
0579-0144 – VS Form 16-3
0579-0213 – VS Form 16-3

0579-0245 – VS Forms 16-3, 17-129
0579-0393 – VS Form 16-3
0579-0055 – VS Form 17-129
0579-0218 – VS Form 17-129
0579-0228 – VS Form 17-129
0579-0473 – VS Form 17-129

PPQ:
0579-0049 (PPQ 587, 585, 588, 586, 546)
0579-0054 (PPQ 526, 525)
0579-0088 (PPQ 526)
0579-0207 (PPQ 526)
0579-0346 (PPQ 586)
0579-0076 (PPQ 621)

BRS:
0579-0085 – APHIS 2000

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   ☐ Cell Tower Records (e.g.,   ☐ Network Communication
Preferences (e.g., Security   Logs, User Location, Time)   Data
Level, Sharing Options,
Ringtones)

Medical /Emergency Information

☐ Medical/Health   ☐ Mental Health   ☐ Disability Information
Information   Information

☐ Workers' Compensation   ☐ Patient ID Number   ☐ Emergency Contact
Information   Information

Specific Information/File Types

☐ Personnel Files   ☐ Law Enforcement   ☐ Credit History Information
                          Information

☐ Health Information   ☐ Academic/Professional ☐ Civil/Criminal History
                          Background Information   Information/Police Record

☐ Case Files   ☐ Security   ☐ Taxpayer Information/Tax
                          Clearance/Background Check   Return Information

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

The data was originally collected directly from individuals applying for permits.

2.2.1. How is the information collected?

No new information is collected in the system. The information was collected from the applicant through the e-permits system which is arranged in a series of workflow steps for both the customer (applicant) and the USDA APHIS employee and other agencies involved in the review and decision-making process regarding permit issuance.

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 commercial or publicly available data is used.

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

There are no checks being done as this is an archival system that allows the data to be read only, and no information can be changed or entered into the ePermits Legacy System. Individuals who need corrected permits are directed to the new e-File system, which has replaced ePermits for new permits moving forward.

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?

Not applicable.

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

Not applicable.

2.6.   **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: There is a risk that PII will be maintained that is not necessary for the purpose of this system.

Mitigation: The system maintains only the minimum amount of PII needed to store legacy permits.

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 ePermits Legacy application does not collect information and will provide USDA APHIS users with the ability to search historical permits and application related data. The data is being maintained to be able to research current applications that have not expired. Also, this data is maintained in case legal issues arise and certificates need to be referenced for the Biotechnology Regulatory Services (BRS).

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 technology is being used to conduct electronic searches, queries, or analysis to discover or locate a predictive pattern or anomaly.

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

Follow the format below:

Privacy Risk: There is the risk of PII data being accessed by unauthorized personnel and of it being used outside of its intended purpose.

Mitigation: Role-based security and access rights are implemented to protect the confidentiality of information. Role-based security ensures that users are only allowed to view information within the system that their work role dictates. Also, users must use their e-Authentication which accesses ePermits Legacy. Auditing of user access is performed quarterly to ensure users still need access to the application. BRS, PPQ, and VS personnel determine who has access to the system and what roles they are assigned. The system owner or designated representative approves access to the system. All USDA employees take USDA information security awareness training annually, which includes the proper and improper uses of information.

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 PIA serves as notice to the public about the types of information in ePermits Legacy and how it is used. Because it is an archival system, no new collections of information are taking place.

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

There are no options available to individuals moving forward, as new data is no longer being collected. Any new information collections occur in the e-File system.

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

Follow the format below:

Privacy Risk: There is a risk that individuals are unaware that their historical permit information continues to be maintained in the ePermits Legacy archival system.

Mitigation: This PIA describes the information collected in ePermits Legacy and how the USDA uses it. It is posted publicly on the USDA's website.

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.

Section 5: Data Retention

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

5.1.   What information is retained and for how long?

- Records maintained by Plant Protection and Quarantine (PPQ): DISPOSITION: Temporary. Cut off at the end of the fiscal year in which permit expires. Delete/destroy 10 years after cutoff.

- Records maintained by Veterinary Services or Biotechnology Regulatory Services: DISPOSITION: Temporary. Cut off at the end of the fiscal year in which permit expires. Delete/destroy 7 years after cutoff.

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: Animal Comprehensive Electronic Permit System number N1-463-09-008.

5.3.   **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: There are risks related to long term retention of PII, both from a minimization and integrity standpoint. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity.

Mitigation: ePermits Legacy only retains the minimal amount of information needed to meet the business requirements. The application is an archival application and has read only access and it follows the established procedures to destroy information as annotated within the approved NARA schedule. Access for internal users is audited on a quarterly basis to ensure that only active users with need-to-know have access to the system.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1.   With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Information is not shared internally.

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

Follow the format below:

Privacy Risk: There is a risk of exposing PII to unauthorized personnel.

Mitigation: The information with the internal organizations is electronically shared between systems. System users must log in to see this data which minimizes the impact of exposing PII to unauthorized personnel.

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 may be shared with entities identified in the SORN associated with this system. The data that is shared is mentioned in 2.1. The information is shared via encrypted email, and the file is password protected.

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

Follow the format below:

Privacy Risk: External sharing with permitted entities in the SORN creates risks of unauthorized access, data breach during transmission and secondary disclosure without APHIS consent.

Mitigation: The risk is mitigated by ensuring that the personnel that request the information are authorized to receive the information and a password is sent separately in an encrypted email to the requesting officer, documenting all sharing activities and conducting periodic reviews to ensure continued appropriateness of external sharing arrangements.

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?

No external individuals and/or organizations will be provided with direct access to the ePermits Legacy Application or ePermits Legacy data. However, individuals may submit Freedom of Information Act (FOIA) requests to APHIS via the online portal or to:

APHIS Privacy Act Officer, Legislative and Public Affairs, APHIS, 5601 Sunnyside Ave. Ap-740, Beltsville, MD 20705.

Fax: (301) 734-5941

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

Users cannot directly modify ePermits legacy data, but they can request corrections by submitting a Privacy Act request as stated in 7.1. ePermits Legacy data will be read only as this is an archival system.

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

Individuals are notified at the point of collection of information, through this PIA and the SORN identified in Section 1.3.

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

Formal redress is provided.

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

Follow the format below:

Privacy Risk: There is a risk that individuals will not be able to access or update their information or be aware of how to do so.

Mitigation: Individuals may file FOIA requests as listed above to access their information. If there is a correction that needs to be made on a current permit in ePermits Legacy, they can submit a request for correction.

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 system provides technical safeguards to prevent the misuse of data and APHIS conducts continuous monitoring of the system to ensure the technical safeguards are in place. The technical safeguards include, but are not limited to:

Encryption: Encryption is implemented to secure data at rest and in transit for the application, which makes the data unreadable to unauthorized users.

Access Control: Role/feature-based access is used to ensure staff only receive access to limited data that they need only for their job responsibilities. Access for internal users is audited on a quarterly basis to ensure that only active users with a need-to-know have access to the system and it is read-only access.

Authentication: Access to the system and session timeout is implemented for this application (by eAuthentication). This process requires a password plus an additional form of authentication and logs users out after a period of inactivity.

Audit: Logging is implemented for this application (date/time of the last record update, user that last updated the record) and can be reviewed if information is mishandled.

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

The individual programs determine what level of access is required for a new program user. The application uses role-based access control (RBAC) to limit what specific data individuals and programs can access. Access requires supervisor approval. There is only read access available to all users.

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

All requests are made through the program representative for BRS, PPQ, and VS.

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

All users are required to take annual information security awareness training that educates them on the proper handling and protection of PII. This is required for both initial and continued access to the system.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 9/17/2025

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:_____

David S. Neitch
ePermits Legacy System Owner
Marketing and Regulatory Programs (MRP)
U.S. Department of Agriculture

Signed:_____

Angela Cole
Assistant Chief Information Security Officer (acting)/Chief Privacy Officer
Marketing and Regulatory Programs (MRP)
U.S. Department of Agriculture