Comprehensive Electronic Permitting System (ePermits)

Privacy Impact Assessment

Policy, E-Government and Fair Information Practices

- Version: 2.1
- Date: November 3, 2022
- Prepared for: Marketing and Regulatory Programs

United States Department of Agriculture

Privacy Impact Assessment for the

Comprehensive Electronic Permitting System (ePermits)

August 18, 2022

Contact Point

Patricia Somervell
USDA MRP APHIS
(301) 851-2183

Reviewing Official

Tonya Woods
APHIS Privacy Act Officer
United States Department of Agriculture
(301) 851-4076

Abstract

This Privacy Impact Assessment is for the Comprehensive Electronic Permitting System (ePermits). ePermits provides a web-based tool that enables the public to apply for, check status of application(s), and receive APHIS permits on-line. This PIA is being conducted to determine the potential impact of the data which is collected via ePermits.

Overview

ePermits consists of a set of secure Web-based interfaces to an Oracle database. It includes a permit application interface that supports the entry, update, submission, and tracking of APHIS permit applications by the public. It also contains an interface that supports regulatory processing and issuance of said permits by APHIS staff.

In short, ePermits:

- Provides a Web-based tool that enables the public to apply for, check status of application(s), and receive APHIS permits on-line.
- Supports the electronic issuance of permits.
- Enables APHIS users and officials in DHS to obtain rapid verification of the authenticity and accuracy of an import permit.
- Standardizes the public interface to the APHIS permitting process.
- Enhances the integrity and efficiency of the APHIS permitting process.
- Supports on-line credit card payments through Pay.gov.

ePermits supports three APHIS programs -- PPQ, BRS and VS. This Privacy Impact Assessment addresses the data, uses, and functionality for ePermits.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

- Name, address (including mailing address), telephone number (including work and home numbers), email address, and organization name.
- Destination addresses for shipments of regulated articles, including contact name and phone number.
- For APHIS permits staff who signs permits, the system uses a digital image of the handwritten employee signature to allow this to be printed on the permit.

1.2 What are the sources of the information in the system?

Information for permit applications is input by permit applicants (importers, import brokers, and researchers). Based on the information provided by applicants, APHIS ePermits staff in BRS, PPQ and VS draft permit conditions/restrictions.

1.3 Why is the information being collected, used, disseminated, or maintained?

The purpose of collecting data in ePermits is to collect information related to the application for a permit, fees associated with permits, and to track status information relating to issuance of a permit.

1.4 How is the information collected?

The information is collected by the applicant through the e-permits system which are 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.

1.5 How will the information be checked for accuracy?

Applications are checked for completeness based on requirements defined by APHIS. Some completeness checks are automated, and some are manually built into the workflow process. For example, there are required fields in the system where the permittee must enter data before proceeding to the next page of the application.

Manual verification involves the following steps:

- The APHIS reviewer confirms that all information was received and is complete.
- If information is missing, they can request more information as required.

Data collected from USDA sources is checked for completeness and accuracy in accordance with USDA policies and procedures. Many steps within the workflow require automatic review by another APHIS user to verify its accuracy.

Accuracy is also confirmed based on the fact that the applicant, which is the source of the PII, completes the request for a permit.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The data collected in ePermits is authorized under USDA APHIS regulatory policy and through the approval of the OMB forms which ePermits represents electronically 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)

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The information collected when viewed as a whole, could identify individuals and their activities with regards to APHIS permitting. This information is protected through various levels of security and policy. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view information about others can do so. Auditing of user access is performed quarterly to ensure users still need access to ePermits. Role-based security includes the use of USDA e-Authentication services, which provides user authentication.

Section 2.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The purpose of collecting data from an individual is to collect information related to the application of a permit, fees associated with permits, and to track status information relating to issuance of a permit.

Data will also be used to manage and issue permits and notifications; perform inspections, investigations, and permit-related activities; prepare permits, letters, and other documents; generate reports to evaluate quality control and effectiveness of the program (Note that these reports may include privacy data such as name and address); determine if the action requested in the permit application would be additionally subject to other Federal or State authorities; and facilitate and account for payments.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Business Intelligence (BI) tools are used to generate reports.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Not Applicable. The system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

This information is protected through various levels of security and policy. The system itself is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so.

Data is encrypted while in transport and while at rest. ePermits utilizes eAuthentication to protect access to the system.

Section 3.0 Retention

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

3.1 How long is information retained?

Paper and electronic records will be retained in accordance with disposition authority N1-463-09-8 and Disposal Authority N1-463-96-1 for Item 3029a: Release and Movement Permits and Notifications records and Item 3032a Data Monitoring records. The established records retention schedule is currently being updated. The established timeframes are thirty years for Biotechnology Regulatory Services (BRS), ten years for Plant Protection and Quarantine (PPQ) and seven years for Veterinary Service (VS). (https://www.aphis.usda.gov/library/records/downloads/SS.pdf)

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Role-based security includes the use of USDA e-Authentication services, which provides user authentication and ensures that only authorized personnel have access to the data and to the data that the assigned role is associated.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information is shared with users across the USDA that have a need to know such information to perform the agency's mission. Data is shared across PPQ, VS, and BRS business lines, as well as with corresponding agencies such as IES, Plant Inspection Stations, FSIS, and other USDA HQ and Field agencies as appropriate.

4.2 How is the information transmitted or disclosed?

Information is transmitted electronically directly through the online interface, email and reporting. Role-based access determines the data that can be seen by the individual. For example, based on a user's role, they may view a limited subset of information contained within the system based on their need for that data to perform their duties.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The sharing of data through email is a risk and it is mitigated by sending emails with encryption to protect it during transmission. Additionally, the email is only sent to personnel with a need-to-know in accordance with ePermits processes. Data in the system is accessible to authorized ePermits users, managers, system administrators, database administrators, and other employees with appropriate access rights. Not all data will be accessible by any user; functionality and access is determined and controlled by user roles. Data being transmitted on the internet is a risk. This risk is mitigated as data is encrypted as it traverses the network along with data at rest being encrypted.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state, and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Permit information, to include name, address, phone number and email address, are shared with DHS CBP so that CBP can confirm the validity of permits and compliance to permits conditions when inspecting shipments at the port of entry. Draft permits and substantiating application attachments are shared with State Plant Health Officials. State Plant Health officials review draft permits against state regulations and approve the permits or recommend changes to permitted conditions or permitted articles.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

The information shared outside the Department is compatible with its original collection as it is used directly to monitor and enforce the regulations governing the issuance of permits. The outside agencies use the information to assist the USDA in protecting and enforcing their policies at the various ports of entry across the United States and its territories. This sharing is covered by the APHIS Comprehensive Electronic Permitting System (ePermits) SORN.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information is shared through controlled user access as defined by system requirements. For example, based on a user's role, they may view a limited subset of information contained within the system based on their need for that data to perform their duties. The further away from the issuing agency the role is, the less information a user is typically granted. Agencies outside the USDA have the least amount of access to collected data. The communication protocol that ePermits utilizes is encrypted (https), which ensures protection of the data as it is transmitted.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The privacy risks with external sharing are unauthorized access or disclosure. This is mitigated by utilizing encryption and role-based access for external users with direct access.

By policy, individuals are only able to access the information they need to perform their duties and should not share the information with anyone unless specifically authorized. No reports are shared externally.

Section 6.0 Notice

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

Yes, a SORN is required. The SORN that supports this system is USDA/APHIS-10, APHIS Comprehensive Electronic Permitting System (ePermits) - 73 FR 23406. USDA has set up a web site to provide an additional location to view published PIA's and SORN's at: https://www.usda.gov/privacy-policy.

6.2 Was notice provided to the individual prior to collection of information?

Yes, A privacy notice appears when the customer starts an application for a permit. Also, a link to the ePermits Privacy Act Statement is on the footer of every screen in ePermits.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Yes.

6.4 Do individuals have the right to consent to uses of the information? If so, how does the individual exercise the right?

Yes, the ePermits system and its activities provides privacy notice to individuals so that they understand the consequences of their decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

ePermits applicants "opt in" to the collection of their PII in ePermits to submit their permit application. A privacy act notice pops up once the customer selects a permit to start the application process. Also, a link to the ePermits Privacy Act Notice is on the footer of ever screen in ePermits. The APHIS SORN provides the written consent of the

individual for the disclosure of a record about an individual(s). There are no risks as all users are aware of the collection, use, and dissemination of PII.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

All requests for access to records must be in writing and should be submitted to the APHIS Privacy Act Officer, 4700 River Road, Unit 50, Riverdale, MD 20737; or by facsimile (301) 734–5941; or by email APHISPrivacy@usda.gov. In accordance with 7 CFR 1.112 (Procedures for requests pertaining to individual records in a record system), the request must include the full name of the individual making the request; the name of the system of records; and preference of inspection, in person or by mail. In accordance with 7 CFR 1.113, prior to inspection of the records, the requester shall present sufficient identification (e.g., driver's license, employee identification card) to establish that the requester is the individual to whom the records pertain. In addition, if an individual submitting a request for access wishes to be supplied with copies of the records by mail, the requester must include with his or her request sufficient data for the agency to verify the requester's identity.

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

Correcting inaccurate information may be done via the point of contact in section 7.1

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

They are notified via the system of records notice and individuals would need to follow the procedures listed in 7.1.

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

Redress is provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

No privacy risks are associated with the available redress procedures. The redress procedures were developed based on the requirements of the Privacy Act.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Each program approves access and roles in the system. User access to data is restricted and is based on the role of the user. Applicants see only the data related to their own permit applications. APHIS ePermits staff view only information within their department. CBI is restricted to authorized users. The capability of each system role is documented in the ePermits system documentation. The process for approving roles is documented in the helpdesk procedures and the System Security Plan (SSP).

8.2 Will Department contractors have access to the system?

Yes. Only specifically authorized Department contractors have access to the system. Those individuals must first obtain relevant security clearances along with specific authorization to access information at various levels.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

The annual USDA Security Awareness training is the privacy training that is provided to all Federal employees and contractors who access the information system. The standard USDA warning banner must also be acknowledged and accepted before logging into the system.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, a full assessment and authorization has been completed. The most recent Authority to Operate was granted on 4/26/2019 and is in the process of renewing at this time.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

In addition to the positive user identification through the USDA ICAM Shared Services system and the application of specific and restrictive user roles within the system, periodic role review audits are performed by the agency to ensure users have only the roles necessary to complete their official duties. Physical access control, firewalls (access control), and intrusion detection systems prevent unauthorized access and misuse of data.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The privacy risks associated with ePermits during information sharing are limited to unauthorized sharing and mishandling of shared data. Auditing is enabled at the database and web application level which creates logs showing which data was accessed by which users. Data is also encrypted to ensure secure transmission. The system utilizes role-based access and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

This system is a web-based information system that collects and tracks status information relating to issuance of a permit.

9.2 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23

"Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

The system does not use third-party websites or applications.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

N/A

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require

either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Does the system use web measurement and customization technology?

No, the system does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A

Signed copy kept on file.