Privacy Impact Assessment
ePermits

Technology, Planning, Architecture, & E-Government

- Version: 1.7
- Date: April 17, 2019
- Prepared for: USDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

Comprehensive Electronic Permitting System (ePermits)

April 17, 2019

Contact Point
Camille Chapman
USDA APHIS
(301)851-2246

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

Danna Mingo
MRP Privacy Compliance Officer
Information Security Branch
United States Department of Agriculture
(301) 851-2487

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. In March 2014, ePermits completed an independent Certification and Accreditation. 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?

Customer – Customers enter permit application information, check the status of permit applications, and view permit responses. Customers also collaborate with the APHIS Permit Staff to verify accuracy of the permit and to ensure all requirements are met.

The system uses the following information about customers:

- Name, address (including mailing address), telephone number (including work, FAX and home numbers), email address, and organization name and job function.
- Name, quantity, country of origin and intended use of regulated articles (organisms and materials) to be imported.
- Destination addresses for shipments of regulated articles, including contact name and phone number.
- Planned dates and ports of entries for shipments, planned quantities of permitted articles in shipments.
- For permits that require fee payments by credit card, the system has an interface with the pay.gov system. Credit card payments are processed with Pay.gov. The last four digits of credit card numbers are stored in ePermits.
- For BRS permit applications, the applicant may declare that some permit application information is Confidential Business Information (CBI), a designation allowed under Section (b)(4) of the Freedom of Information Act, which exempts from disclosure certain types of information related to trade secrets and commercial or financial information.

The system uses the following information about employees:

- Name, address (including mailing address), telephone number (including work, FAX and home numbers), email address, and organization name and job function.
- For APHIS permits staff who signs permits, the system uses a digital image of the handwritten employee signature for printing on the permit.

Other - State regulatory agencies review permit applications, and enter comments about draft permit conditions. Agricultural Inspectors from the U.S. Customs and Border Protection use ePermits to view permits and confirm the validity of permits.

The system uses the following information about other:

Name, address (including mailing address), telephone number (including work, FAX and home numbers), email address, and organization name and job function.

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 permits staff in BRS, PPQ and VS draft permit conditions/restrictions, route a copy of the permit application and draft permit conditions to one or more State regulatory officials to review and add comments. Finally, APHIS permits staff review comments from the States and issue a final permit.

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

The principle purpose of collecting data in ePermits 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 and the final outcome.

1.4 How is the information collected?

The information is collected through online pages which are arranged in a series 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 in ePermits that all information was received and is complete.
- If information is missing, they can use ePermits to request more information as required.

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

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:
    - The Virus-Serum-Toxin Act (21 U.S.C. 151-159), 9 CFR Subchapter E, Parts 102 to 124.
    - 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: Introduction of Organisms and Products Altered or Produced Through Genetic Engineering; OMB 0579-0085
- 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)
  - Honey Bee Act (7 U.S.C. 281)
  - Agriculture Bioterrorism Act (7 USC 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 obtained 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.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The principle 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 and the final outcome.

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 (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?

Cognos is used for ad hoc reporting.

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.

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. The established records retention schedule is currently being updated. Some records considered as permanent will be maintained in accordance with NARA requirements.

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

Yes

The data retention schedule is currently being updated.

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

The retention period is in line with standard retention schedules for similar data and is long enough that any likelihood of having issues associated with the archiving or disposal of data is minimal.

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

4.2 How is the information transmitted or disclosed?

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.

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 information shared 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. By policy, individuals are only to access the information they need to perform their duties, and should not share the information to anyone unless specifically authorized.

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?

Information is shared to agencies such as DHS CBP agents who work to support the APHIS mission at various ports of entry.

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 which use the information 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 an appropriate routine use in APHIS - 10 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. All access to data in the ePermits system is restricted through HTTPS.

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

The information shared 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. By policy, individuals are only to access the information they need to perform their duties, and should not share the information to 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 Was notice provided to the individual prior to collection of information?

Prior to logging into ePermits and providing information the user is required to acknowledge a privacy and security notice. This page also provides additional links that provide the user further information on their rights.

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

Individuals are generally not required to provide the information collected, however they must provide the data should they wish to legally obtain a permit through USDA APHIS.

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

The individual does not have the ability to consent (or opt out) of particular uses of the information collected in the system. If they acknowledge the collection of the information, they are providing the authorization to use the information for the purposes of reviewing and issuing regulatory decisions regarding permit issuance.

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

Individuals are provided sufficient notice as to their rights and are required to positively acknowledge receipt of this notice prior to using the ePermits system. There is no way for a user to provide the information, without first acknowledging they understand the information is being collected and used for the purposes of reviewing and issuing regulatory decisions regarding permit issuance.

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?

The procedures that allow individuals to gain access to their information is documented in the System of Records Notice located at the following link:

https://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records

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

Customers may access information by submitting a Freedom of Information Act (FOIA) request to: APHIS FOIA Office, 4700 River Road, Unit 50, Riverdale, MD 20737 or email the FOIA Officer at FOIA.Officer@aphis.usda.gov.

The USDA Privacy Policy can be located at the following URL: https://www.usda.gov/privacy-policy. Information about FOIA/Privacy Act requests can be found at: https://www.aphis.usda.gov/aphis/resources/foia/ct_how_to_submit_a_foia_request

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

They are notified via the system of records notice.

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

N/A

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 redress available. 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 data related to their own permit applications. APHIS permits staff view only information within their department. CBI is restricted to authorized users. Select agent permit data is restricted to authorized users.

8.2 Will Department contractors have access to the system?

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 USDA Security Awareness annual training is the privacy training that is provided to all Federal employees and contractors who access the information system.

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

Yes, a full C&A has been completed.

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

In addition to the positive user identification through eAuthentication and the application of specific and restrictive user roles within the system, periodic role review audits are performed by the agency in order to ensure users have only the roles necessary to complete their official duties.

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?

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.

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?

The project is a web based information system on a standard technology platform.

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.

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

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

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

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?

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

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

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

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

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

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?

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

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)?

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

10.10 Does the system use web measurement and customization technology?

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?

The system does not use web measurement and customization technology.

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.

Not Applicable as the system does not use third party websites, applications, or web measurement and customization technology.

Approval Signature

MICHAEL GREGOIRE

Digitally signed by MICHAEL GREGOIRE
Date: 2019.04.18 09:23:21 -04'00'

Michael Gregoire
Information System Owner
Plant Protection and Quarantine
Animal and Plant Health Inspection Service
United States Department of Agriculture

PRESTON GRIFFIN

Digitally signed by PRESTON GRIFFIN
Date: 2019.04.18 16:20:47 -04'00'

MRP CISO or MRP ISSPM
Marketing and Regulatory Programs
United States Department of Agriculture

TONYA WOODS

Digitally signed by TONYA WOODS
Date: 2019.04.24 16:01:48 -04'00'

Tonya Woods
APHIS Privacy Act Officer
Animal and Plant Health Inspection Service
United States Department of Agriculture