Privacy Impact Assessment
APHIS eFile

Technology, Planning, Architecture, & E-Government

- Version: 1.3
- Date: March 7, 2019
- Prepared for: USDA APHIS

United States Department of Agriculture

Privacy Impact Assessment for the

APHIS eFile System

March 7, 2019

Contact Point
John Golden
Animal and Plant Health Inspection Service
301 851-2688

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

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

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Animal and Plant Health Inspection eFile System. The APHIS eFile system 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 APHIS eFile.

Overview

The Animal and Plant health Inspection Services (APHIS) of the United States Department of Agriculture (USDA) is charged with protecting the health and value of American agriculture and natural resources from the introduction of destructive plant and animal diseases and pests. These efforts support the overall mission to protect and promote agriculture and natural resources.

APHIS eFile consist of a set of secure Web-based interfaces on the SalesForce platform, which include 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.

This PIA is being created for the APHIS eFile which is a cloud provided solution.

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 (including full name, mother's maiden name, maiden name of the individual, nickname or alias, business name)
- Telephone number (including work, Fax and home numbers)
- Address Information (include mailing address, email address, and organization name and job function)
- Date/Place or birth

- Name, quantity, country of origin and intended use of regulated articles (organisms and materials) to be imported.
- Photographic image/identifying characteristics
- Proposed Articles to be permitted
- Risk mitigation requirements
- Compliance agreements and inspection reports
- Shipment Information (including country of origin)
- Handwriting or an image of the signature
- Destination addresses for shipments of regulated articles, including contact name and phone number.
- Miscellaneous identification numbers (national accreditation number and state license numbers.
- Planned dates and ports of entries for shipments, planned quantities of permitted articles in shipments.
- For Biotechnology Regulatory Service (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 APHIS eFile 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?

Permit applications submitted by permit applicants (importers, import brokers, and researchers). Comments provided by APHIS permits staff and state officials in order to issue a permit.

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

The principle purpose of collecting data in APHIS eFile 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 an online application.

The decision-making process is an online series of steps followed by the APHIS customer (applicant), APHIS employee, and other government agency staff who are required to review the information regarding permit issuance.

1.5 How will the information be checked for accuracy?

The system includes required fields where the applicant must enter data before proceeding to the next page of the application. The applicant has an opportunity to review their information and must certify that the information was entered correctly prior to submission.

APHIS employees, and other government agency officials are required to review the information regarding permit issuance. Manual verification involves the following steps:

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

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

Dog permitting is covered under The Animal Welfare Act (AWA). The BRS permits are covered under The Plant Protection Act.

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 can

view information. [*Note:* Due to the level of development customization in the cloud platform, identified PII cannot be encrypted.] Auditing is being performed and system audit logs are being reviewed for suspicious activity.

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?

Inherent Salesforce platform tools are used.

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?

Dog Permitting:

Paper and electronic records will be retained in accordance with disposition authority NI-463-09-9 which is currently being updated. Some records considered as permanent will be maintained in accordance with NARA requirements.

Limited Animal Welfare Act electronic records are maintained permanently on a separate secured server for trend analysis and maintained by NARA.

BRS Records are proposed to be retained for 30 years.

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

Dog permitting disposition authority in being updated and pending approval.

BRS records retention schedule is pending approval.

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 system must maintain a disposition authority and without approval to destroy records the data will be maintained longer than needed. This has negative impacts on the privacy risk of the data. Once the NARA disposition is approved the system owner will ensure records are destroyed according to the authority.

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?

At this time APHIS eFile does not share information internally.

4.2 How is the information transmitted or disclosed?

N/A

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.

N/A

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 Department of Homeland Security (DHS) Custom and Border Protection (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 USDA 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 that 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 and live dog permitting is covered under pending APHIS 8 SORN that has been updated and pending approval.

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. The user's role, is limited to the information needed to perform their duties.

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 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. In addition, limited information is sent to CBP through secure file transfer based on role-based permissions.

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?

Yes, prior to logging into APHIS eFile 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?

No, applicants must provide the information in order to obtain a permit.

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.

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 APHIS eFile system. Users are not permitted to submit an application without first acknowledging they understand the information is being collected and used for the purposes of reviewing and issuing regulatory decisions regarding permit issuance. A privacy statement will appear at the bottom of the system home page. The public is also made aware through the publication of the SORN(s).

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?

APHIS implements a Rules of Behavior (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the USDA implementation of User Security Awareness training which is provided annually by the Department. In addition, APHIS provides personally identifiable Information Lite training via AgLearn.

Safeguards:

All APHIS eFile users are required to complete USDA's registration process called eAuthentication, a system that enables individuals to obtain user-identification accounts that allow password protected access to certain USDA web-based applications and services through the Internet. The web-based service identifies and validates USDA customers before they can access APHIS eFile. Role-based security and access rights are implemented to protect the security of the information. Additionally, the APHIS eFile security plan includes management, operational, and technical controls to prevent misuse of data by system 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 MRP Privacy Program requires all APHIS users to take the USDA Protection of PII training on an annual basis. Names are submitted to the MRP Privacy Compliance Officer and the training is added to their AgLearn account.

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

Yes.

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

All users are required to have an individual user account to the application system. Both MRP and DSC perform active monitoring and oversight of account management best practices using account management policy and active reporting.

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. In addition, the system is designed to track all changes made against the lifetime of a record (version history). Data is retained a minimum of 5 years, but not to exceed 30 years. Length of retention is governed by the type of record.

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?

APHIS eFile is a web based information system on a cloud base system

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

The system resides on the Salesforce cloud platform. The information is being managed by a contractor and storage and protections are not in the control of the agency. However, the platform is FedRAMP approved.

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?

Not Applicable

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

Not Applicable

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

Not Applicable

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?

Not Applicable

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

Not Applicable

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

Not Applicable

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?

Not Applicable

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)?

Not Applicable

10.10 Does the system use web measurement and customization technology?

Not Applicable

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

Not Applicable

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

Approval Signature

LAURA LEWANDOWSKI
Digitally signed by LAURA LEWANDOWSKI
Date: 2019.03.13 11:21:37 -04'00'

John Golden
System Owner – APHIS eFile
Animal and Plant Health Inspection Service
United States Department of Agriculture

PRESTON GRIFFIN
Digitally signed by PRESTON GRIFFIN
Date: 2019.03.14 16:50:02 -04'00'

MRP CISO/MRP ISSPM
Animal and Plant Health Inspection Service
United States Department of Agriculture

TONYA WOODS
Digitally signed by TONYA WOODS
Date: 2019.03.19 16:04:47 -04'00'

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