Privacy Impact Assessment
Plant Protection and Quarantine (PPQ) Service Portal

Animal and Plant Health Inspection Services

- Version: 1.2
- Date: June 25, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

PPQ Service Portal

June 25, 2020

Contact Point
Brandon Hieskill
APHIS
(301) 851-2261

Reviewing Official
Preston J. Griffin
Acting Chief Information Security Officer
APHIS MRP IT
United States Department of Agriculture
(301) 851-2502

Abstract

This Privacy Impact Assessment is for the Animal and Plant Health Inspection Services (APHIS) Plant Protection and Quarantine (PPQ) Service Portal.

The PPQ Service Portal is a cloud-based application built upon the Salesforce.com Platform-as-a-Service (PaaS) platform. It allows users to request, execute, and track work requests and projects created by Center for Plant Health Science and Technology (CPHST). Data and Analytics, Regulatory Analysis and Development (RAD), and Plant Epidemiology and Risk Analysis Laboratory (PERAL) staff using a consolidated system-wide application developed on a common Salesforce platform.

Overview

The purpose of the PPQ Service Portal is a work request tracking and project management system that enables APHIS PPQ employees to collaborate effectively. This system supports PPQ's ability to deliver data and analytic products to PPQ customers and their stakeholders to aid their data-driven decision making by providing a request intake forum, project tracking system, final product repository, and customer feedback loop. Everything is built on the Salesforce Force.com Platform-as-a-Service (PaaS). There is an interconnection to the SpingCM system outside of the boundary of the PPQ Service Portal, due to the library size limitation of 10 megabytes and 25 megabytes within Salesforce. Legal authority to operate the program or system is the Plant Protection Act (7 USC 7711, 7712, and 7714), and Sections 10404 through 10407 of the Animal Health Protection Act.

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?

The PPQ Service Portal is an internal system used for tracking APHIS employees work requests and a knowledge base for their analytic products. The application keeps a history of all internal requests – which are tied to Salesforce records in the system. The PII data that is collected by PPQ Salesforce Portal is USDA employees name and work email address.

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

The information in the PPQ Service Portal comes from a myriad of databases including USDA APHIS systems Agricultural Quarantine Activity System (AQAS), Agricultural

Risk Management (ARM), Integrated Plant Health Information System (IPHIS), and Automated Commercial Environment (ACE)/International Trade Data System (ITDS), and multiple data repository/archival sources.

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

The information is used for analysis, violations, and investigations.

1.4 How is the information collected?

The information is being collected through a manual process of input into the system.

1.5 How will the information be checked for accuracy?

For every application within the PPQ Service Portal, the business workflow requires that a team leader and additional reviewer signs off at every step in the process from project creation, initial assignment, and final proofing\delivery.

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

Legal authority to operate the program or system is the Plant Protection Act (7 USC 7711, 7712, and 7714), and Sections 10404 through 10407 of the Animal Health 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 following are risks for the PPQ Service Portal Application:
- Unauthorized system access through the USDA OCIO eAuthentication system.
- Improper identification through the USDA OCIO eAuthentication system.

Common mitigation is provided by the USDA-OCIO-eAuthentication application, which provides user authentication for the PPQ Service Portal application. Role-based access control granted by PPQ Service Portal administrators using eAuthentication to verify user authentication and set permissions within the PPQ Service Portal application.

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 information is used for analysis, violations, and investigations.

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

No tools are used to analyze the data once it reaches the Salesforce application. The data (reports) will be tagged with metadata tags for searching/archival purposes, but otherwise will reside in a folder-like structure (document library or repository).

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

Public and commercial data can be used based on the initial request type by the customer. The determination is based on the type of project request and associated audience selected. The audience options are Federal Government (APHIS), State\local government, international government, Academia, or industry.

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.

Role based access control is in place within the application to protect data from unauthorized access, and eAuthentication is used for identification and authentication into the PPQ Service Portal application.

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?

The PPQ Service Portal aligns with PPQ's data retention policy based on source of the analytic information. The data retention schedule is being developed at this time and is covered by POA&M 27085.

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

No. POA&M 27085 covers this deficiency.

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 access control is in place within the application to protect data from unauthorized access, and eAuthentication is used for identification and authentication into the PPQ Service Portal application.

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 sharing and purpose is based on the type of project request and associated audience selected. The audience options are Federal Government (APHIS), State\local government, international government, Academia, industry. No PII is shared.

4.2 How is the information transmitted or disclosed?

The information is transmitted (disclosed) by way of email attachments through SpringCM or directly downloaded\uploaded from Salesforce.

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.

PPQ Service Portal information is available internally to APHIS PPQ personnel that are granted permission to access the PPQ Service Portal application via eAuthentication. The SpringCM system, on which some data could be stored outside the boundary of the Salesforce.com PaaS, allows for file-level encryption on emailed data.

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?

APHIS PPQ is tracking the number of requests and types of work requests that are being completed internally by their data analytic units (Data Analysis and Risk Targeting). No information is being shared outside of USDA.

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.

No personally identifiable information is being shared.

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

No personally identifiable information is being shared.

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 on 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 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?

No.

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

No.

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

No.

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.

No notice is provided and the 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 on 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 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?

There are no procedures for individuals to gain access to their information.

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

None.

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

There are no procedures for individuals to gain access to their information.

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

A System of Record Notice (SORN) will be on file with the proper authority. The SORN is being developed and covered by POA&M 27088

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

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 user requiring access to the APHIS PPQ Service Portal must request access through the program manager. Once access is approved, a user is created within the Salesforce Platform-as-a-Service (PaaS) that corresponds to an eAuthentication (eAuth) account. By using an eAuth login, users can then access the PPQ Service Portal application in their assigned role.

8.2 Will Department contractors have access to the system?

No.

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

Every APHIS employee is required to take annual training on PII. If the course is not completed annually, then access is revoked until the course is completed.

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

Certification and Accreditation has not yet been completed, but is underway as of September, 2015.

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

The Service Portal team will mandate auditing on all workflows, training requirements, and user role controls every quarter. Additionally, all users are required to have an individual account.

8.6 <u>Privacy Impact Analysis</u>: 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 on 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 APHIS Plant Protection and Quarantine (PPQ) Service Portal allows users to request, execute, and track work requests and projects created by Center for Plant Health Science and Technology (CPHST), Data and Analytics, Regulatory Analysis and Development (RAD), and Plant Epidemiology and Risk Analysis Laboratory (PERAL) staff using a consolidated system-wide application developed on a common Salesforce platform. The PPQ Service Portal is a work request tracking and project management system that enables APHIS PPQ employees to collaborate effectively. This system supports PPQ's ability to deliver data and analytic products to PPQ customers and their stakeholders to aid their data-driven decision making by providing a request intake forum, project tracking system, final product repository, and customer feedback loop.

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

No technology is employed that may raise privacy concerns.

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?

3rd party websites are not used within the APHIS PPQ Service Portal application.

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

3rd party websites are not used within the APHIS PPQ Service Portal application.

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

3rd party websites are not used within the APHIS PPQ Service Portal application.

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?

3rd party websites are not used within the APHIS PPQ Service Portal application.

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

3rd party websites are not used within the APHIS PPQ Service Portal application.

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

3rd party websites are not used within the APHIS PPQ Service Portal application.

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?

3rd party websites are not used within the APHIS PPQ Service Portal application.

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)?

3rd party websites are not used within the APHIS PPQ Service Portal application.

10.10 Does the system use web measurement and customization technology?

No.

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?

Not applicable; web measurement and customization technology is not used within the APHIS PPQ Service Portal application.

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; 3rd party websites are not used within the APHIS PPQ Service Portal application.

Responsible Officials

Brandon K. Hieskill

Project Manager, APHIS MRP IT

United States Department of Agriculture

301-851-2261

Brandon.K.Hieskill@aphis.usda.gov

Approval Signature

PRESTON GRIFFIN Digitally signed by PRESTON GRIFFIN
Date: 2020.07.24 15:22:59 -04'00'

Preston J. Griffin
Acting Chief Information Security Officer (CISO)
APHIS MRP IT
United States Department of Agriculture

JANELLE JORDAN Digitally signed by JANELLE JORDAN
Date: 2020.07.06 13:56:23 -04'00'

Tonya Woods
APHIS Privacy Act Officer
United States Department of Agriculture

NICOLE RUSSO Digitally signed by NICOLE RUSSO
Date: 2020.07.06 14:57:48 -04'00'

Nicole L. Russo
PPQ Salesforce Portal Information System Owner
APHIS PPQ
United States Department of Agriculture