Privacy Impact Assessment Phytosanitary Certificate Issuance and Tracking (PCIT)

- Version: 1.3
- Date: August 3, 2018
- Prepared for: USDA OCIO TPA&E

Privacy Impact Assessment for the

Phytosanitary Certificate Issuance and Tracking (PCIT)

August 3, 2018

Contact Point
Darlene Rush
APHIS, BISSM, PMO
(301) 851-2161

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

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

Abstract

The Phytosanitary Certificate Issuance and Tracking System (PCIT) is a web application. It facilitates the creation and processing of plant export applications with the intent of generating an export certificate. The PIA is being conducted to document the data collection, use, retention, sharing, access, and customer protection.

Overview

- Phytosanitary Certificate Issuance and Tracking System (PCIT), APHIS PCIT's purpose is to facilitate the creation and processing of plant export applications (OMB Form 572) with the intention of generating an export certificate (OMB 577, 578,579). The export certificate, known as the Federal Phytosanitary Certificate is created to allow entry of plants or plant products into a foreign country. The certificate certifies to the foreign plant protection service that the shipment has been inspected and was found to conform to the phytosanitary import requirements of that country. In addition, the certificate attests that the shipment was appropriately treated for or free from quarantine plant pests and pathogens and is practically free from other injurious pests. It relates to the mission by providing a service to citizens in alignment with international affairs and commerce that helps to protect the health and value of American agriculture.
- The information in the system includes the data that exporters enter to create an application for the export of agricultural goods to foreign countries. The information entered includes consignee, commodities, and destination country. The exporter only has visibility into their organization's information. It is though not likely, the exporter or consignee information could be a personal address and/or phone number. An exporter can choose not to participate in the program. If they do, it understood that the information is collected for the processing Phytosanitary Certificates only. If an exporter chooses not to participate, manual certificates can still be processed by the Federal or State cooperator. Though the information is still manually collected.
- A typical transaction conducted on the system would involve an applicant who accesses PCIT for the purpose of exporting plant products. They would go to PCIT website and to pay for their certificates the applicant would click a link within the PCIT website and the applicant would be redirected to Treasury's Pay.Gov. No financial data is kept in PCIT. The only information transmitted to PCIT is the Org ID and the amount deposited in the organization account and this is completed through a secure TLS connection between Pay.gov and PCIT. An ISA has been established to address this connection. PCIT is connected to the USDA e-Authentication platform for its users. Federal and state officials use PCIT to adjudicate applicant data and certify that the plants or plant products were inspected prior to leaving the U.S. port and conform to any phytosanitary entry requirements the importing country has set.

- Information sharing conducted by PCIT includes State and County cooperators which act as surrogates to APHIS with roles in issuance of phytosanitary certificates that have access to the data within their organizations.
- PCIT's module includes the Phytosanitary Export Database (PExD) which houses the export requirements for plants and plant products to foreign countries.
- PCIT was granted the Authority to Operate (ATO) effective June 25, 2010.
- In March 2012, a pilot system named Veterinary Export Health Certificate System (VEHCS) was deployed to support Veterinary Services (VS) in creating and endorsing animal health certificates (HC) for exporting cattle, swine and poultry to Canada and poultry to Guatemala. VEHCS enables Accredited Veterinarians (AV) to create and submit on-line HC, and Veterinary Medical Officials (VMO) to review and endorse the HC.
- VEHCS was developed based on PCIT architectural framework. It operates on PCIT hardware and shares the Weblogic application server with PCIT. VEHCS has its own database that stores certificates data. Pilot users access the application via the PCIT URL.
- In June 2013, PCIT login page was modified to become a common APHIS application log in portal to further enhance and integrate VEHCS, and enable VEHCS users to self-register.
- PCIT was granted a new Authority to Operate (ATO) effective August 20, 2016.

1 Section 1.0 Characterization of the Information

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

Information collected, used, disseminated and maintained in PCIT includes consignee, commodities, and destination country. The exporter enters data including their company name, address and phone number. The exporter or consignee information could be a personal address and/or phone number. The information is required as part of the certificate issuance process. The Accredited Certifying Official (ACO) name and duty station is collected as part of the information that will be displayed on a certificate. The ACO may choose to have his signature captured through a manual process. The ACO fills out a form, with signature and the signature image is scanned and stored in the PCIT database as part of the ACO's record.

A similar process is employed in VEHCS. The Accredited Veterinarians, who are certified by VS, can obtain a Level 1 eAuthentication account, and then register with VEHCS. The pertinent information being collected include

- Veterinary Clinic (* indicates required data)
  - Business Name
  - First Line Address*
  - Second Line Address
  - City*
  - State*

  - Zip Code*
  - Phone Number
  - Fax Number
  - Email Address
- Accredited Veterinarians (* indicates required data)
  - First Name*
  - Middle Initial
  - Last Name*
  - Name and Credentials to be displayed on the Health Certificate*
  - Email Address
  - License Number(s)* State(s)* Expiration Date(s)*
- Attach additional license data if necessary.
  - Accreditation Number*
  - Expiration Date*
  - State(s)*

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

Industry information provided by exporters on commodities to be shipped

Federal, State and Local Officials: information needed to certify shipment

The AV information is provided by the AV during the self-registration process.

The VMO information is provided by the VEHCS business program to be loaded into the system.

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

The information is being collected, used, disseminated or maintained to create an application for the export of agricultural goods to foreign countries. ACO name is required on a certificate. ACO signature is also required and they may choose to do a manual signature or electronic image.

Similarly for VEHCS, The AV information is being collected, used, disseminated or maintained to create an HC for the export of animals to foreign countries. VMO name is required on a certificate.

1.4 How is the information collected?

Exporters enter the information in the system via the internet (web access). The ACO may choose to have his signature captured through a manual process. The ACO fills out an ACO signature form, with signature and the signature image is scanned and stored in the PCIT database as part of the ACO's record.

On VEHCS system, the AVs enter the information in the system via the internet (web access). The VMO information is provided by the VS business program and is uploaded to the system by a background database script or entered by VS through VEHCS via internet.

1.5 How will the information be checked for accuracy?

Reference tables are being used. Edit checks are available on data fields when possible. Automated edit checks at the field level and a final check on the application to be submitted is done when the user signifies the application is complete. Checks for completeness are included in the actual issuance of the certificate by the certified official to ensure applicable information has been captured. Only persons that are valid ACO's or VMOs as defined by PCIT have the privilege to sign or endorse certificates. ECS' are responsible to ensure that ACO's are current. The VS Headquarter management is responsible to ensure VMOs 'data is accurate and current.

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

The Plant Protection Act (7 U.S.C. 7701 et seq.)

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.

Risk of exposure of address and/or telephone number of the exporter or consignee are minimal. No address/phone is explicitly designated as personal. These data are "company" information. Access to data is granted by organization and only the exporter has access to its data and that includes the consignee information. Consignees designate who is receiving the shipped commodities.

Only the ACO of name can access and use their electronic signature image. This is built into the PCIT roles software.

The VEHCS system is designed to maintain confidentiality for the AVs. Their information is securely stored in the VEHCS database. They can only access HC data which they create.

2 Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The data collected is for the creation of Phytosanitary certificates needed to export plant products outside of the U.S. The data may also be used to track national export activities and help in predicting market trends for the future. Specifically the data will be used to evaluate application data and issue certificates, schedule and perform inspections, investigations and

phytosanitary related activities, and generate reports to evaluate quality control and effectiveness of the Program. An ACO signature (electronic image or hand written) are required on all certificates issued.

For VEHCS, the data collected is for the creation of the animal health certificates needed to export live animals outside of the U.S. The data may also be used to track national export activities and help in predicting market trends for the future. Specifically the data will be used to evaluate application data and issue certificates, schedule and perform inspections, investigations and veterinary related activities, and generate reports to evaluate quality control and effectiveness of the Program.

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

COGNOS, a Business Intelligence (BI) tool is used to analyze the data and produce reports that evaluate quality control and effectiveness of the program. COGNOS is the designated APHIS/PPQ BI tool and integral to operation, much the same as Oracle DBMS, or general operating elements of the general infrastructure.

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

N/A

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.

To gain access to the PCIT/VEHCS systems all users are required to have an USDA e-Authentication account. This a 2 step process where the user name identifies the user and the password authenticates that the user is in fact who he claims to be. Once an individual gains initial access to PCIT/VEHCS, there are 2 options:

1. Create a New Organization (typically done by the organization administrator) or Join an existing organization.
2. To join an existing organization, the person must be invited and will receive a unique PIN from the organization administrator.
3. Thus only individuals belonging to an organization has access to the data
4. For use of the ACO signature, only the ACO of name can access and use their electronic signature image. This is built into the PCIT roles software.

3 Section 3.0 Retention

3.1 How long is information retained?

The proposed disposition authority for PCIT records are as follows pending NARA approval:

- Commodity data includes identifiers and characteristics. Disposition: twenty years.
- Certificate data includes fee, applicant, consignee, treatment, and importing country requirements. Disposition: twenty years.
- Attachment data includes all supporting documentation. Disposition: five years.

VEHCS records are permanent until the records have been scheduled..

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

Approval is pending. The MRP400 has been submitted to Agency records officer for submission to NARA for 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 retention period mentioned above does not pose a risk to the data. The system and its data is protected and access controls are in place to protect the integrity of the data.

4 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 within APHIS to provide reports about the effectiveness of the Program. Typically these are reports generated by or at the request of the PCIT or VEHCS program office which delineates commodity shipments. There is no data sharing between other APHIS systems at this time.

4.2 How is the information transmitted or disclosed?

Information is transmitted by the generation of reports using the COGNOS business intelligence tool.

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.

There is no PII data and no privacy risks associated with reporting. Neither address/phone nor ACO/VMO name or signature data is shown on any documents other than Phytosanitary Certificates or Health Certificates which are required for the export of plant commodities to foreign trade partners.

5 Section 5.0 External Sharing and Disclosure

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

1. To certain State and county government regulatory officials to evaluate applications; schedule and perform inspections and related phytosanitary activities; generate phytosanitary certificates; investigate complaints about noncompliance with phytosanitary requirements; and evaluate program quality and effectiveness;
2. To certain Federal agencies, pursuant to the International Trade Data System Memorandum of Understanding, consistent with the receiving agency's authority to collect information pertaining to transactions in international trade;
3. To certain foreign governments concerning applications for phytosanitary certificates involving that country;
4. To the appropriate agency, whether Federal, State, local, or foreign, charged with responsibility of investigating or prosecuting a violation of law or of enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and either arising by general statute or particular program statute, or by rule, regulation, or court order issued pursuant thereto;
5. To the Department of Justice when: (a) the agency, or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States, is a party to llitigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which the records were collected;
6. For use in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when:

a. the agency, or any component thereof; or
b. any employee of the agency in his or her official capacity; or
c. any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or
d. the United States, is a party to litigation or has an interest in such litigation, and the agency determines that use of such records is relevant and necessary to the litigation; provided, however, that in each case, the agency determines that disclosure of the records to the court is a use of the information contained in the records that is compatible with the purpose for which the records were collected;

7. To appropriate agencies, entities, and persons when:
   a. the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;
   b. the agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, a risk of identity theft or fraud, or a risk of harm to the security or integrity of this system or other systems or programs (whether maintained by the agency or another agency or entity) that rely upon the compromised information; and
   c. the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the agency's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;
8. To contractors engaged to assist in administering the program. Such contractors will be bound by the nondisclosure provisions of the Privacy Act;
9. To USDA contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends, or anomalies indicative of fraud, waste, or abuse; and
10. To the National Archives and Records Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

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.

Yes, it is covered by the APHIS-13 Phytosanitary Certificate Issuance and Tracking (PCIT) SORN.

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

No data is shared with the state a county personnel as they are given access to PCIT to perform their required duties. A secure trusted server connectivity through the use of installed x.509 SSL digital certificates, as well as the specification of IP addresses for required firewall configurations. Each connection is then further validated through an API application login and password handshake to establish the encrypted HTTPS connection over TLS 1.2 transport security protocols. Once the secure connection is established, the transmission of electronic phytosanitary certificates occur to the International Trade Data System.

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

When sharing information with external organizations, the same specifications related to security and privacy that are in place for USDA APHIS employees are also applied to these outside Departments or Agencies. Access to PCIT data is governed by the "need-to-know" criteria and requires that the receiving entity demonstrate the need for the data before access or interface is granted. The reason for the exchange/interface request and the implications on privacy are two factors included in both the initial and ongoing authorization, the Interconnectivity Security Agreement (ISA) negotiated between APHIS PPQ and the external agency seeking to access to PCIT data. In general terms, the ISA specifies the conditions that govern the limitations associated with the use of the data, while the ISA specifies the data elements, format and the interface utilized during an electronic exchange.

6 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. Section 6.0 Notice

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

Yes, the SORN will serve as the official notice. The collection of the information is required to be able to export commodities and make sure that the shipment is compliant with all the applicable laws and regulations.

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

No, because the individual needs to provide all the information required to process the Phytosanitary certificate to be able to export their commodity.

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, because if the user does not provide the information they will not be able to obtain the certificate to be able to export their commodity.

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.

APHIS has issued a new System of Records Notice (SORN), APHIS-13 Phytosanitary Certificate Issuance and Tracking (PCIT) in conjunction with his PIA. Notice is also provided through the publication of this PIA on the Internet. Additionally, USDA has set up a web site to provide an additional opportunity to view published PIA's.

7 Section 7.0 Access, Redress and Correction

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

Any individual may obtain information from a record in the system that pertains to him or her. Requests for hard copies of records should be in writing, and the request must contain the requesting individual's name, address, name of the system of records, timeframe for the records in question, any other pertinent information to help identify the file, and a copy of his/her photo identification containing a current address for verification of identification. All inquiries should be addressed to the Freedom of Information and Privacy Act Staff, Legislative and Public Affairs, APHIS, 4700 River Road Unit 50, Riverdale, MD 20737-1232.

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

Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager at the address identified in the system or records notice. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

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

Notification for correcting information in the system can be found in the SORN.

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.

N/A

8 Section 8.0 Technical Access and Security

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

Users must access the system through documented e-Authentication procedures.

8.2 Will Department contractors have access to the system?

Yes

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

PCIT/VEHCS are public web based systems. Training is the responsibility of user's organizations. State and county officials and their contract personnel are provided the required training by their organizations.

All APHIS officials must take the annually security awareness training provided by USDA and sign a Rules of Behavior (ROB).

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?

Built in audit information on data changes are provided per PCIT software. Oracle auditing is provided as agreed between PPQ and NITC. NITC controls the database auditing. A user can only access its organizations data. A user can belong to only one organization.

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?

For ACO name and voluntary electronic signature image; this has been addressed in sections above. For address/phone, this has been address above.

9 Section 9.0 Technology

9.1 What type of project is the program or system?

PCIT/VEHCS is a centralized web based application.

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

No

10 Section 10.0 Third Party Websites/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 PCIT/VEHCS systems do not utilize any 3rd party websites.

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

None

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?

Yes, the system is reviewed annually to demonstrate compliance to OMB M-10-23.

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?

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.

Data is not accessible through 3rd party websites and/or applications.

Authorizing Officials

Christian B. Dellis

System Owner

Animal Plant Health Inspection Service

United States Department of Agriculture

Rajiv Sharma

Information System Security Program Manager

Animal Plant Health Inspection Service

United States Department of Agriculture

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