Privacy Impact Assessment

Phytosanitary Certificate Issuance and Tracking (PCIT) & Veterinary Health Export Certificate System (VEHCS)

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: November 15,2022
- Prepared for: Marketing and Regulatory Programs

Privacy Impact Assessment for the

Phytosanitary Certificate Issuance and Tracking (PCIT) &
Veterinary Health Export Certificate System (VEHCS)
November 15, 2022

Contact Point

Alisa D. Robinson
MRP IT PMO
(301) 851-3605

Reviewing Official

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

Abstract

This Privacy Impact Assessment is for the Phytosanitary Certificate Issuance and Tracking System (PCIT) and Veterinary Export Health Certificate System (VEHCS) system web applications. The applications facilitate the creation and processing of plant export applications with the intent of generating a phytosanitary export certificate and the creation of animal health certificates (HC) for exporting live animals and germplasm. This PIA is being conducted to determine the potential impact of the data which is collected via PCIT and VEHCS.

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 or 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 possible, but not likely, the exporter or consignee information could be a personal address and/or phone number. Although the use of PCIT is not mandated, the 750,000 certificates issued each year by PCIT. An exporter choosing to participate in the program understands that the information is collected for the processing of Phytosanitary Certificates only.
- PCIT is connected to the USDA e-Authentication platform for user validation and log in.
- Applicant transactions conducted are for the purpose of exporting plant products. 1) They go to PCIT website to create/submit applications for certificates. 2) They use a link within PCIT to be redirected to Treasury's Pay.gov site to establish/replenish an account balance to be debited when their certificates are issued. Upon successful completion of a financial transaction at Pay.gov, Pay.gov sends the transaction amount to PCIT. PCIT adds this amount the account balance of the applicant. No financial data is kept in PCIT. The only information transmitted to PCIT is the applicant's Org ID and the amount. The communication between PICT and Pay.gov is completed

through a secure TLS connection. An ISA has been established to address this connection.

- Federal, state and county officials use PCIT to adjudicate application 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 complement APHIS staff. State and County officials with roles supporting the issuance of phytosanitary certificates have access to the data within their organizations.
- PCIT includes the Phytosanitary Export Database (PExD) which houses the export requirements for plants and plant products to foreign countries.
- Veterinary Export Health Certificate System (VEHCS) was deployed to support Veterinary Services (VS) in creating and endorsing animal health certificates (HC) for exporting live animals and germplasm. VEHCS enables Accredited Veterinarians (AV) to create and submit HC's, and APHIS Veterinary Medical Officials (VMO) to review and endorse them.

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?

Information collected, used, disseminated, and maintained in PCIT includes exporter and consignee data including their company name, address, and phone number. The exporter or consignee information could be a personal address and/or phone number. 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 signature may be 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 pertinent information being collected include the following all of which is entered through the VEHCS GUI.

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)*, Expire Date(s)*
- Accreditation Number*, State(s)*, Expire Date(s)*

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

PCIT applicant information is input by applicants/exporters during the self-registration process and is self-maintained. PCIT Federal, State and County ACO information needed to certify shipment is input and maintained by specially designated PCIT program users.

VEHCS AV information is provided by the AV during the self-registration process and is self-maintained. VEHCS VMO information is input and maintained by the VEHCS business program.

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 plant and plant products to foreign countries. The ACO information collected is the ACO name which is required on a certificate.

Similarly, for VEHCS, the AV and VMO information is being collected, used, disseminated, or maintained to create a HC for the export of live animals and germplasm to foreign countries. AV and VMO names are 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 entered by VS through VEHCS via internet.

1.5 How will the information be checked for accuracy?

The Export Certification Specialist (ECS) are responsible to ensure that ACO data is accurate and current. The VS Headquarter management is responsible to ensure VMO data is accurate and current.

Accuracy is also confirmed based on the fact that the applicant, which is the source of their PII, completes the application for a certificate or the health certificate.

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.

While risk of exposure of PII exists, it is minimal. Role-based access control is implemented to protect the confidentiality of information. Access to data is granted by organization and only the exporter has access to its data and that includes the consignee information. Role-based security includes the use of USDA e-Authentication services, which provides user authentication. This access is reviewed annually, at a minimum, to ensure users continue to require access.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The data collected is for the creation of phytosanitary certificates needed to export plant products 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 handwritten) 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. 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.

VEHCS database integrates with the VS Data Integration Services (DIS). VS DIS creates reports for VS internal use only and such reports may be stored on an internal Tableau server, within DIS itself, or be downloaded as a file for internal uses.

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.

Access to data is based on roles assigned on a need-to-know premise. Role-based security and access rights are implemented to protect the confidentiality of information. Role-based security includes the use of USDA ICAM Shared Services, which provides user authentication.

Data is encrypted while in transport and while at rest.

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 records are indefinite until a retention schedule has been approved.

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

No. A retention period has not been formally established for data at this time. We are working with the APHIS records management officer to establish a data retention schedule to reduce the amount of data maintained in the system.

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

There is minimal risk associated with the length of time data is retained. This is mitigated as access to data is based on roles assigned on a need-to-know premise. Role-based security and access rights are implemented to protect the confidentiality of information. Role-based security includes the use of USDA ICAM Shared Service, which provides user authentication. Data is encrypted while in transport and at rest which ensures an extra layer of security on the data. Auditing of user accounts are completed also which ensures only appropriate personnel have access to the data.

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?

When necessary, exporter information is shared due to FOIA requests or investigations initiated by Investigative and Enforcement Services (IES).

4.2 How is the information transmitted or disclosed?

Information is transmitted electronically directly through the online interface, email, and reporting. Reports are typically output as electronic files and provided to the requestor in support of their mission.

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

The sharing of data through email is a risk and it is mitigated by sending emails with encryption to protect it during transmission. Additionally, the email is only sent to personnel with a need-to-know in accordance with PCIT/VEHCS processes. Data in the system is accessible to authorized PCIT/VEHCS users, managers, system

administrators, database administrators, and other employees with appropriate access rights. Not all data will be accessible by any user; functionality and access is determined and controlled by user roles. Data being transmitted on the internet is a risk. This risk is mitigated as data is encrypted as it traverses the network along with data at rest being encrypted.

Section 5.0 External Sharing and Disclosure

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

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

(1) Designated 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) Designated 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) Designated 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 litigation 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.

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 that has been published at the following link: https://www.usda.gov/home/privacy-policy/system-records-notices

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 communication protocol that PCIT/VEHCS utilizes is encrypted (https), which ensures protection of the data as it is transmitted.

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

The privacy risks with external sharing are unauthorized access or disclosure. This is mitigated by utilizing encryption and role-based access for external users with direct access. Access to data is based on roles assigned on a need-to-know premise. Role-based security and access rights are implemented to protect the confidentiality of information.

By policy, individuals are only able access the information they need to perform their duties and should not share the information with 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 Does this system require a SORN and if so, please provide SORN name and URL.

- Yes, a SORN is required. The SORN that supports this system is USDA/APHIS-13, Phytosanitary Certificate Issuance and Tracking System - 78 FR 37775 - June 24, 2013. USDA has set up a web site to provide an additional location to view published SORN's at: https://www.usda.gov/home/privacy-policy/system-records-notices.

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

Yes. The SORN or PIA is the official notice of why PII is being collected and it can be located at https://www.usda.gov/home/privacy-policy/system-records-notices.

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

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 plant/plant product or animal.

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

No, because the information obtained from the user is to be able to obtain the certificate to be able to export their plant/plant product or animal and this only a single use when it comes to inputting the information.

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

Applicants "opt in" to the collection of their PII by creating an electronic authentication account within USDA ICAM Shared Services and logging into PCIT/VEHCS to submit their application or health certificate. The PCIT/VEHCS SORN provides the written consent of the individual for the disclosure of a record about an individual(s). All users are aware of the collection, use, and dissemination of PII.

Section 7.0 Access, Redress and Correction

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

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

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

Every PCIT and VEHCS user has the ability in the respective systems to maintain their descriptor data such as name. Also, if the user establishes an organization, they can also maintain business address, email, and phone number.

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

Correcting inaccurate information may be done via the point of contact in section 7.1. All users can self-correct their information.

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?

Redress is provided.

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

No privacy risks are associated with the available redress procedures.

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 and AV see only the data related to their own applications. APHIS PCIT/VEHCS staff view only information within their duty station or field office location. The capability of each system role is documented in the PCIT/VEHCS system documentation. The process for approving roles is documented in the PCIT/VEHCS Access Control Account Management Procedures document.

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 annual USDA Security Awareness training is the privacy training that is

provided to all Federal employees and contractors who access the information system. The standard USDA warning banner must also be acknowledged and accepted before logging into the system.

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

Yes, The Authority to Operate (ATO) was granted on 8/24/2021.

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

Periodic role review audits are performed by the agency to ensure users have only the roles necessary to complete their official duties. DISC provides physical access control, firewalls (access control), and intrusion detection systems to prevent unauthorized access and misuse of data. Below are events captured within audit logs:

- Create user and create date
- update user and update date

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

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

Section 9.0 Technology

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

9.1 What type of project is the program or system?

PCIT/VEHCS is a centralized web-based application that issues certificates relevant to the exporting of plants/plant products and animals.

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

No.

Section 10.0 Third Party Websites/Applications

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

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

Yes.

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

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

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

N/A

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

N/A

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

N/A

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

N/A

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

N/A

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

N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Does the system use web measurement and customization technology?

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

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

N/A

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

N/A

Signed copy kept on file.