Privacy Impact Assessment
Agriculture Quarantine Activity System (AQAS)

◄ Version: 1.0

◄ Date: November 14, 2011

◄ Prepared for: USDA OCIO TPA&E

USDA

United States Department
of Agriculture

Privacy Impact Assessment for the

Agriculture Quarantine Activity System (AQAS)

November 14, 2011

<u>Contact Point</u>
John Dirocco
APHIS/PPQ
301-734-7342

<u>Reviewing Official</u>
Tonya Woods
APHIS Privacy Officer
United States Department of Agriculture
(301) 734-5267

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

Abstract

The Agricultural Quarantine Activity System (AQAS) records quarantine activities conducted by Department of Homeland Security (DHS), Customs and Border Protection (CBP), and APHIS Plant Protection and Quarantine (PPQ) employees at the ports of entry into the United States. AQAS also records trade-related activities conducted inside the US. The PIA is being conducted to describe the Personally Identifiable Information (PII) being captured by AQAS, how it is used and the security controls in place to protect the PII commensurate with identified risk.

Overview

The Agricultural Quarantine Activity System (AQAS) records quarantine activities conducted by Department of Homeland Security (DHS), Customs and Border Protection (CBP), and APHIS Plant Protection and Quarantine (PPQ) employees at the ports of entry into the United States. AQAS also records trade-related activities conducted inside the US. AQAS aids the free flow of agricultural goods into the country by collecting agricultural risk data that ultimately help to minimize the impact of quarantine activities on trade. All five of the subsystems of the AQAS system are interrelated, web-based, and share a common platform:

1.   Agricultural Quarantine Inspection Monitoring (AQIM)

The AQIM system provides a systematic approach to determining the risks of cargo approaching the port by collecting specific data about randomly sampled shipments. AQIM then analyzes the data to identify the high-risk criteria and to target inspections accordingly. Ports are selected for random sampling of agricultural shipments using PPQ280 data.

AQIM – Ship Monitoring Pathway: The Ship Monitoring pathway includes data entry functions for both the Ship Arrival and the Passenger (inspection) records. Ship Arrival and Passenger (inspection) records are closely linked. A Ship Arrival record can be associated with zero, one, or more Passenger (inspection) records, but each Passenger (inspection) record can be associated with exactly one Ship Arrival record.

2.   Emergency Action Notification (EAN)

The EAN system tracks the issuance of Emergency Action Notifications (PPQ Form 523). PPQ Form 523 is generated by DHS and PPQ officers throughout the country when an actionable violation is detected related to prohibited pests and agricultural products found in cargo, market places, or domestic sites.

3.   Pest Identification (Pest ID)

The Pest ID system tracks pest interceptions in agricultural commodities at the port and beyond the port, domestically. The Pest ID system records the identification of quarantine pests made by PPQ and cooperating identifiers found during the following events:

- Agricultural Quarantine Inspections (AQI)
- Smuggling Interdiction and Trade Compliance (SITC) activities

- Domestic Surveys
- Emergency Domestic Program (EDP) events.

The Pest ID system also facilitates trade by expediting the reporting of Urgent AQI Interceptions and Domestic Detections. The pest data are used for risk assessments, trade negotiations, port resource allocation, and local program analysis.

4. PPQ280 System

The PPQ280 system tracks the volume and disposition of commodities (e.g., fruits, vegetables, cut flowers, propagative material, lumber, and certain miscellaneous products) imported or transiting through a port. The PPQ280 tracks the final disposition of the commodity; the number of shipments; and the commodity's quantity, type, and country of origin.

The PPQ Plant Inspection Stations use the PPQ264 portion of the PPQ280 system to track quarantined propagative plant material. The PPQ264 data are also used to document inspection results by shipment and to generate notices to state Departments of Agriculture about plant material to be shipped to their states. Both the PPQ280 and the PPQ264 data are used for risk analysis.

5. Work Accomplishment Data System (WADS)

The WADS system tracks work activities related to agricultural inspections at US ports. WADS codes are designed to report on activities such as the number of foreign arriving passengers or foreign cargo, number of inspections conducted, or number of clearances conducted. Other WADS codes report on the outcomes of inspection activities, such as number of Quarantine Materials Intercepted (QMIs), reportable pests, violations, or treatments. The purpose of the WADS system is to enable APHIS to set risk-management priorities and to make staffing recommendations. WADS data are analyzed in conjunction with other AQAS data for risk analysis. For example, WADS data are compared with AQIM data to help increase each port's efficiency on agricultural-pest risk targeting.

6. PPQ287 (Mail Interception)

Form 287 is currently used for reporting the interceptions of certain materials found in mailed packages.

The PPQ287 Mail Interception Database provides a means to do the following in the event of a mail interception:

- Electronically generate a notification (Form 287) to be provided to the intended recipient ("addressee") and the sender (the "addressor"). This notification will indicate that an unauthorized Material—animal products, animal byproducts, plants, plant products, plant pests, or soil—was removed from the mail package, and why.

- Record the regulatory action that Customs and Border Protection took when intercepting the mail.

- Provide a means to prepare monthly and quarterly reports.

- Centralize the management of all mail interceptions into a single database. This will greatly improve the accessibility and quality of data gathered for intercepted mail.

AQAS Data Warehouse

In addition to the AQAS production system, the AQAS Data Warehouse provides a limited number of power users with the capability to perform ad-hoc queries on large, national datasets for each AQAS subsystem (e.g., AQIM, EAN, Pest ID, PPQ280/264, and WADS).

Currently the AQAS Data Warehouse is implemented at the National Information Technology Center (NITC) in Kansas City, Missouri. The production AQAS system is also hosted at NITC.

To gain access to the AQAS Data Warehouse, the user must get approval from either the Director of PPQ-Quarantine Policy and Analysis Support or the Director of PPQ-Plant Safeguarding and Pest Identification. Users must be approved for national access; that is the data are not restricted by location. Typically AQAS production system users are assigned to a limited number of locations; however, data warehouse users can see data for all locations.

The data warehouse tables are refreshed from the AQAS production data every business day at 2 a.m.

The AQAS Data Warehouse also does the following:

- Reduces the processing load on the AQAS production system.
- Allows users to create reports of their own design without having to write programs.
- Optimizes the AQAS data for information and analysis.
- Provides a quicker response time for reporting than the AQAS production system.

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 Agricultural Quarantine Activity System (AQAS) tracks data about quarantine activities conducted by Department of Homeland Security (DHS) Customs and Border Protection (CBP) and APHIS Plant Protection and Quarantine (PPQ) employees at the ports of entry into the United States. The data collected in the AQAS system contain a wide range of trade events including ship arrivals, quarantine activities, invasive pest interceptions, and

other commodity exclusion actions. Additionally, it contains sampling results to statistically validate the quality of the import inspection pathways.

AQAS also records trade-related activities conducted inside the US. Both the EAN and Pest ID subsystems track domestic activities, including actionable violations related to agricultural products and pest interceptions found in domestic sites.

The AQAS system collects the following data:

- Customer Data: PPQ280 and EAN collect the owner/consignee and shipper information. PPQ264 collects the name, business address, email address and business phone number of state contacts who are state and university employees.
- Employee Data: The AQAS system collects the user name (first initial, middle initial, and last name), email address, and assigned location name for DHS and APHIS employees.
- Other Data: Commodity import, agricultural inspection data, pest data.

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

Sources of data come from both USDA Animal and Plant Health Inspection Service (APHIS) - Plant Protection and Quarantine PPQ and DHS Customs and Border Protection (CBP) employees and authorized personnel.

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

The principal purpose for the information to be collected, stored, disseminated or maintained is to allow USDA and DHS to make risk-based decisions about the admissibility of certain commodities from other countries and their transfer within the U.S.

1.4   How is the information collected?

The information is collected from USDA and DHS employees manually inputting data into automated forms created in each AQAS module.

1.5   How will the information be checked for accuracy?

There is a quarterly meeting with joint representation of DHS-CBP and USDA-APHIS-PPQ personnel to review the AQIM, WADS, PPQ280, and EAN data of each period for accuracy, relevance, timeliness, and completeness.

For PPQ264, data are collected in a timely manner: as shipments are cleared or shortly thereafter. National, regional, and local PPQ staff periodically review the data for accuracy and completeness. The staff also reviews the data to ensure its relevance for the purposes of risk assessment and reporting to the states.

For Pest ID, PPQ identifiers review records for accuracy, relevance, timeliness, completeness, and they correct the data as needed. The PPQ National Identification Staff (NIS) in Riverdale also regularly review Pest ID records (either identified by business system rules or per identifier requests) for accuracy relevance, timeliness, and completeness. The PPQ NIS staff evaluates and updates the data as needed.

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

Public Law 106-224, Plant Protection Act and approved Memorandums of Understanding (MOU) with DHS CBP.

1.7 <u>Privacy Impact Analysis</u>: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

AQAS does not collect privacy data from the public, so the privacy risks are limited to government employees. 128-bit encryption is used for the latest version (v3.3) of Secure Socket Layer (SSL) to protect data being transferred over the wire. System credentials which support system access control are protected using strong one-way hash. System credentials are obscured while users input their credentials to access the system.

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 principal purpose of AQAS is to collect and store data on agricultural goods. These data are used to make risk-based decisions about the admissibility of certain commodities from other countries.

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

Business Intelligence (BI) tools are used to generate reports, trends and graphs. Privacy data is typically not included in the reports, trends and graphs.

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

Commercial or publically available shipping data is used to determine to identify shipments of regulated imported commodities.

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.**

128-bit encryption is used for the latest version (v3.3) of Secure Socket Layer (SSL) to protect data being transferred over the wire. System credentials which support system access control are protected using strong one-way hash. System credentials are obscured while users input their credentials to access the system.

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?**

Currently the information is retained indefinitely.

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

N/A

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. The main risk is the availability of the information and the length of time it would take for users to perform data mining activities due to the breadth of 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?**

If the commodity falls within veterinary circles, then the data would be shared with APHIS-Veterinary Services (VS).

4.2   How is the information transmitted or disclosed?

The information is made available electronically through the AQAS system interface.

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 are no privacy risks to consider through information sharing with APHIS-VS.

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 with DHS CBP for staffing purposes and to allow for DHS to make risk-based decisions about the admissibility of certain commodities from other countries and their transfer within the U.S.

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.

PII is not being shared with DHS.

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

N/A

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

N/A

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, through the user account distribution and management process.

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

No, the information is required to receive user credentials and gain access to the system.

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

Yes, prior to receiving user credentials, an AQAS regional coordinator provides the user role which gives the individual certain rights and access to information.

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.

Notice is provided when users submit a user account form. Risks are mitigated by all users receiving background checks and user information being stored encrypted.

The SORN is being developed and is being managed by POA&M 16399.

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?

AQAS regional coordinators submit a user account form requesting user credentials for an individual. The user is then sent an email with user credentials and a temporary password which requires the user to change upon initial login.

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

Individuals submit a ticket to the AQAS help desk and a help desk analyst assists with correcting the information after receiving approval from AQAS system managers.

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

Yes

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.

There are minimal privacy risks, but the redress approval process mitigates the risks to adequate levels.

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?

AQAS regional coordinators submit a user account form requesting user credentials for an individual. The user is then sent an email with user credentials and a temporary password which requires the user to change upon initial login. The users are documented in a database file.

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?

APHIS requires all system users to take privacy and cybersecurity on an annual basis. The records are stored electronically for verification purposes.

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?

Auditing is enabled at the database and web application level which creates logs which detail objects accessed by users. Role-based access controls are enabled to provide least privilege. 128-bit encryption is used for the latest version (v3.3) of Secure Socket Layer (SSL) to protect data being transferred over the wire. System credentials which support system access control are protected using strong one-way hash. Robust, 12-character, mixed case with special character system credentials are obscured while users input their credentials to access the system.

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 security controls are implemented based on the NIST SP 800-53 security control requirements and have been approved to mitigate risk to an adequate level.

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?

This is a moderate impact, major application which is in the steady state phase of the CPIC life cycle.

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?

N/A

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)?

No

10.10 Does the system use web measurement and customization technology?

No

If so, is the system and procedures 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 all uses of web measurement and customization technology?

No

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

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.
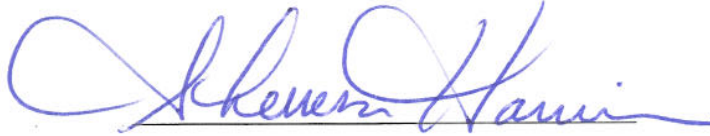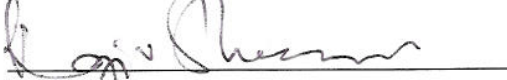
N/A

Responsible Officials

John Dirocco

APHIS-PPQ-ITDC

United States Department of Agriculture

Approval Signature

Sherrena Harrison
System Owner
Animal Plant Inspection and Service (APHIS)
United States Department of Agriculture

Rajiv Sharma
APHIS ISSPM
Animal Plant Inspection and Service (APHIS)
United States Department of Agriculture

Acting APHIS CIO
Animal Plant Inspection and Service (APHIS)
United States Department of Agriculture

Tonya Woods
APHIS Privacy Officer
Animal Plant Inspection and Service (APHIS)
United States Department of Agriculture