Privacy Impact Assessment
Agriculture Quarantine Activity System (AQAS)

- Version: 1.4
- Date: May 11, 2018
- Prepared for: USDA OCIO TPA&E

Technology, Planning, Architecture, & E-Government

Privacy Impact Assessment for the

Agriculture Quarantine Activity System (AQAS)

May 11, 2018

Contact Point
Michael Sileo
APHIS/PPQ
301-851-2059

Reviewing Official
Tonya Woods
APHIS Privacy Act Officer
United States Department of Agriculture
(301) 734-5267

Danna Mingo
Privacy Compliance Officer
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 by products, 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.

7. AQAS Data Warehouse

The AQAS Data Warehouse is a copy of the AQAS database that is used for reporting purposes. 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). The AQAS data warehouse contains a copy of the AQAS data that is optimized for reporting and query purposes.

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.

1 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 input into AQAS by USDA and DHS employees. The source data comes from shipping documents such as manifests, air waybills, and entry documents. Additional information is input into AQAS that reflects the results of inspections performed by USDA and DHS employees.

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 and approved Memorandums of Understanding (MOU) with DHS CBP. In addition, the Plant Protection Act (7 U.S.C. 7701 et seq. and 7 U.S.C. 7781 et seq.); the Honey Bee Act (7 U.S.C. 281 et seq.); and the Animal Health Protection Act (7 U.S.C. 8301 et seq.).

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

AQAS may contain the name and address of an individual under the following circumstances:

- An individual who was issued a From 287 – Mail Interception Notice when a prohibited item was found in international mail package.
- An individual who was the owner of property where a plant pest was found and submitted for diagnostic identification.

AQAS contains an image of the signature of a government employee (currently Murali Bandi, Assistant Deputy Administrator, PPQ) on letters that are generated for National Plant Protection Officers. These letters are generated by AQAS automatically each month and emailed to the appropriate recipient. AQAS users cannot access the letters or the signature image.

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.

The risks associated with the data contained within AQAS are considered Low despite the Moderate classification. The risk is low as the confidentiality, integrity, and availability of the information if compromised will not adversely affect the operations of APHIS or the USDA. The Moderate classification in accordance with FIPS 199 is assigned for the purpose of AQAS containing PII information.

2 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 is 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. The type of data that is available includes inspections, diagnostics, and regulatory actions related to cargo, passengers and international mail entering the US. The primary business intelligence tool is Cognos although users may extract data using Cognos and use other tools such as Microsoft Excel.

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

Commercial shipping documents are used to identify incoming cargo shipments and the type of commodity, quantity and country of origin.

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.

3 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?

Records will be retained indefinitely until appropriate disposition authority is obtained, and records will then be disposed of in accordance with the authority granted.

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

The approval is pending.

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 no additional risk associated with the length of time that AQAS data is retained. Risks are mitigated for historical data using the same controls that are preset for current data. System integrity controls implemented in accordance with NIST 800-53 as defined in the AQAS System Security Plan protect data stored within the AQAS information system.

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?

If the commodity falls within veterinary circles, then authorized persons in APHIS-Veterinary Services (VS) may be given access to query the commodity data in the AQAS data warehouse via Cognos.

APHIS Plant Protection and Quarantine (PPQ) users create Pest Diagnostic Requests and Emergency Action Notifications (EAN's) from within IPHIS system. IPHIS utilizes AQAS web services for Pest Diagnostic Request and EAN functionality. The diagnostic requests and EAN's created from IPHIS are stored in the AQAS database, but can be viewed, edited and printed from the IPHIS system.

The AQAS system connects to the Agriculture Research Service (ARS) SELIS server and uses SFTP to send diagnostic requests from AQAS to SELIS and to receive diagnostic determinations from SELIS to AQAS.

4.2 How is the information transmitted or disclosed?

AQAS data is not transmitted outside of the AQAS database; however authorized internal personnel may be given access to the data via the AQAS application reports or 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 are limited privacy risks with information sharing with APHIS-VS. Risks are mitigated by providing limited access to specific data on a need to know basis. Access controls implemented in accordance with NIST 800-53 as defined in the AQAS System Security Plan define the principles of least privilege and separation of duties. These access controls in accordance with the Rules of Behavior govern the access and use of information within the AQAS information system.

5 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?

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, records maintained in the AQAS system may be disclosed outside USDA as follows:

[1] To DHS CBP and other cooperating Federal or State government employees, or contractors performing or working on a contract, service, grant, cooperative agreement, or other assignment for USDA, when necessary, to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are USDA officials and employees. Specific applications include, but are not limited to, issuing notifications for noncompliance to importers, shippers, property owners, mail recipients or addressees; informing State entities about upcoming plant shipments; using AQIM data to track and analyze various pathways and the commodities entering those pathways into the

United States for purposes of pest risk management; and generating reports to evaluate quality control and effectiveness of the program. Regulated imported commodity (PPQ280) records are generated from the DHS CBP ITDS system and are stored externally from ITDS in XML files on a secure CBP file server. The AQAS system connects to the secure CBP file server each night and uses SFTP to transfer the XML files onto an AQAS server and then loads the records into the AQAS data warehouse. The PPQ280 records are used to report on the volume of imported commodities entering the United States.

[2] To appropriate law enforcement agencies, entities, and persons, whether Federal, foreign, State, Tribal, local, or other public authority responsible for enforcing, investigating, or prosecuting an alleged violation or a violation of law or charged with enforcing, implementing, or complying with a statute, rule, regulation, or order issued pursuant thereto, when a record in this system on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or court order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutive responsibility of the receiving entity;

[3] To the Department of Justice when the agency, or any component thereof, or any employee of the agency in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or the United States, in litigation, where the agency determines that litigation is likely to affect the agency or any of its components, 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;

[4] To a court or adjudicative body in administrative, civil, or criminal proceedings 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 Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records;

[5] To appropriate agencies, entities, and persons when: (a) USDA suspects or has confirmed that there has been a breach of the system of records; (b) USDA has

determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, USDA (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

[6] To another Federal agency or Federal entity, when the USDA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach;

[7] To a Congressional office from the record of an individual in response to any inquiry from that Congressional office made at the written request of the individual to whom the record pertains;

[8] To USDA contractors and other parties engaged to assist in administering the program, analyzing data, and conducting audits. Such contractors and other parties 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 or to the General Services Administration for records management activities 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.

See routine uses.

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

There is no transmission of data. Authorized DHS employees may be given access to AQAS reports or may be given access to Cognos to query AQAS data.

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

There are no privacy risks as information is contained within AQAS and is not transmitted. User access controls are in place which allows disclosure to only authorized DHS employees. Access to AQAS is for purposes of inputting data and generating reports. The information available does not qualify as PII as it includes the following type of data; inspections, diagnostics, and regulatory actions related to cargo, passengers and international mail entering the US.

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.

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

Externally users do not have access to the AQAS information system so they provide the information on their own accord as the information inputted into AQAS is collected via information provided from the following sources:

- An individual who was issued a From 287 – Mail Interception Notice when a prohibited item was found in international mail package.
- An individual who was the owner of property where a plant pest was found and submitted for diagnostic identification.

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

External users do not have access to the AQAS information system. They can decline to provide information by not forwarding information identified in Section 6.1.

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

External users do not have access to the AQAS information system, so the information included was provided by their consent to ship 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.

7 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?

Individuals are contacted by the AQAS Help Desk via e-mail.

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

The Freedom of Information Act allows individuals to make changes to privacy information collected on their behalf. This information may be requested using the information associated by the SORN in the Federal Registrar.

The following conditions define external users who may have privacy information collected on their behalf.

- An individual who was issued a From 287 – Mail Interception Notice when a prohibited item was found in international mail package.
- An individual who was the owner of property where a plant pest was found and submitted for diagnostic identification.

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

The privacy risks associated with the redress available to individuals is minimal. Primarily the risks are associated with external users who have privacy information included as part of the AQAS process. The redress process could be a timely one as it includes multiple resources. However, the risks are accepted by the external user as they choose to provide the information by completing the required forms for shipment. The compromise of information has a Low impact on APHIS and USDA.

Internally, there are zero risks associated with the redress process as the AQAS Help Desk defines a process in which changes can be made directly within the system.

8 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.

The AQAS Risk Assessment indicates that the system contains privacy information in accordance with the Privacy Act. Therefore, controls defined in NIST 800-53 have been implemented to mitigate risks. The following controls are applicable:

- AR-02 – Privacy Impact and Risk Assessment
- AR-05 – Privacy Awareness and Training
- TR-02 – Systems of Records Notices and Privacy Act Statements

Additional, access controls are established to ensure proper authentication and non-repudiation. Each user is required to read and acknowledge the Rules of Behavior prior to receiving account credentials.

9 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 AQAS system is used for data collection and to support the business processes for inspection, diagnostic, and regulatory actions associated with agriculture quarantine activities conducted by DHS and USDA. 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

10 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

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

10.12 1Privacy 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

Authorization From

Terry Morris

System Owner

Animal and Plant Health Inspection Service

United States Department of Agriculture

Rajiv Sharma

Information System Security Program Manager

Animal and Plant Health Inspection Service

United States Department of Agriculture

Tonya Woods

APHIS Privacy Act Officer

Animal and Plant Health Inspection Service

United States Department of Agriculture