Privacy Impact Assessment
AGRICULTURAL RISK MANAGEMENT (ARM)

Policy, E-Government and Fair Information Practices

- Version: 1.3
- Date: April 26, 2022
- Prepared for: Marketing and Regulatory Programs

United States Department of Agriculture

Privacy Impact Assessment for the

AGRICULTURAL RISK MANAGEMENT (ARM)

April 26, 2022

Contact Point

Steven Schafer
USDA APHIS
970-286-5196

Reviewing Official

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

Abstract

The Agricultural Risk Management (ARM) System is a web-based service-oriented system that supports the operational and analytical needs of USDA APHIS Plant Protection and Quarantine (PPQ) and the Department of Homeland Security (DHS) Bureau of Customs and Border Protection (CBP) Agricultural Quarantine Inspection (AQI) programs. It also supports the diagnostic and regulatory action needs of Federal and State domestic activities, predeparture activities and Smuggling Interdiction and Trade Compliance (SITC) activities focused on mitigating the risks associated with invasive species. The ARM System replaces the existing PPQ information technology (IT) system (in particular the Agricultural Quarantine Activity System {AQAS}. The PIA is being conducted because the system is collecting information from the public that is personally identifiable.

Overview

The ARM System is a workflow-based application that provides real-time data entry, tracking and analysis of import shipments processed at PPQ plant inspection stations, along with CBP cargo inspection activity. The major focus of the system is to target those imports that are likely to have pest(s) that introduce risk into the US agriculture. The functional categories under which data falls within the ARM system are Inspections, Diagnostics, and Regulatory Action. In support of the related USDA processes, the ARM System collects data resulting from the inspection of shipments, passengers, mail and pedestrians at U.S. Ports of Entry. This information is collected primarily by CBP agriculture officers and USDA PPQ inspectors. CBP conducts inspections at ports of entry, to include sea, air, and land border crossings. While PPQ inspectors conduct cargo and mail inspections at various Plant Inspection Stations around the country. In addition, the ARM System supports predeparture operations which includes inspections of mail and cargo in Hawaii and Puerto Rico. It also supports the submission of pest interceptions and generation of regulatory actions for both the Smuggling, Interdiction and Trade Compliance and domestic activities. Inspection data includes but is not limited to information about the inspection location, shipper, origin and destination of the shipment, the shipment mode of transportation, and mail recipients and addressees. If pests are detected, information is collected concerning the identification of the pest. Diagnostic requests may be initiated leading to a final identification of the intercepted pest, as well as a determination on the corrective action necessary (such as treatment, destruction, or re- export.). Where noncompliance is determined, notifications are prepared and sent to permit holders, importers, or brokers and mail recipients. Appropriate information is collected in the ARM System to prepare these notices.

Numerous administration and reference data tables are maintained to support lookup and selection of data where needed within the ARM System. This includes taxonomic, commodity, and shipper/consignee information. Also, user role data is maintained to control user access to functionality and data.

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?

- Trade Party location and address information
- Trade Party Point of Contact details (i.e., name, phone number, and email address)
- Shipment and commodity information (i.e., bill of lading number, customs entry number, container number, ship name, airline and flight number, commodity genus/species, country of origin, quantity, destination) from shipping documents and invoices
- Name and address information from mail envelopes and labels
- Acknowledgment of notifications of violations
- Data submitted by persons entering the U.S and filling out CBP traveler entry forms and USDA forms

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

- Shipment and inspection data is input by CBP, and USDA PPQ inspectors based on information from shipping documents, invoices, inspection logs and worksheets
- Automated APHIS Core Message Set are collected from APHIS OMB approved forms that are electronically submitted by filers
- Pest diagnostic data input and treatment recommendations made by USDA employee (PPQ Identifiers, botanists, and plant pathologists)
- Phytosanitary Certificate data, certifications of the details of plant exports from the exporting country, is retrieved from the Phytosanitary Certificate Issuance and Tracking system
- Shared reference data from other APHIS systems

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

- Communicating and analyzing inspection data for shipments, conveyances, and passengers arriving in the U.S.
- Issuing legal notices and non-compliance with regulations
- Providing information to facilitate tracking violators

- Identifying, qualifying, and communicating trends and changes in plant and animal health issues of concern
- Providing information regarding the effectiveness of AQI and the association of pests with the cargo, mail, and passenger pathway.
- Supporting operational and policy planning and decision-making for delivering efficient, effective, and responsive programs; safeguarding American agriculture; and facilitating safe trade.

1.4 How is the information collected?

Where possible information is received electronically by ARM from participating Trade Parties. Electronic sources of information are the Automated Commercial Environment (ACE) and the Phytosanitary Certificate Issuance and Tracking System (PCIT). When information is not received electronically, it is transcribed from documents by PPQ employees.

1.5 How will the information be checked for accuracy?

Inspectors do document reviews of permits, certificates, shipping documents etc. which includes validating the electronic records in the system against paper records. Discrepancies may be identified in the context of USDA and CBP personnel review of the data and they will take action to correct that information, when appropriate. When corrections are made, ARM updates this information immediately and only the latest data is used.

Furthermore, in the event personally identifiable information used by and/or maintained in ARM is believed by the data subject to be inaccurate a redress process has been developed. See Section 7 of this PIA. To the extent information that is obtained from another system is determined to be inaccurate, this problem would be communicated to the appropriate source for remedial action.

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

The Plant Protection Act, 7 U.S.C. § 7701 -7772 and 7 U.S.C. ~ 7781-7786; Honey Bee Act, 7 U.S.C. § 281-286; the Animal Health Protection Act, 7 U.S.C. §8301-8321; and the Security and Accountability for Every Port Act of 2006, 6 U.S.C. ch. 3 § 901 et seq and 46 U.S.C. ch. 701, subch. I § 70101 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.

The risk of PII data being accessed by unauthorized personnel is mitigated 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 e-Authentication services, which provides user authentication. User roles are granted through web-of-trust mechanisms in place.

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.

- Shipment and inspection data is used to validate and verify that all shipments are in compliance with trade regulations.
- Pest diagnostic data is used to determine if shipments require treatments and tomake recommendations regarding the type of treatment that may be required.
- Taxonomic data is used to collect, communicate, and analyze inspection data forshipments, conveyances, and personnel arriving in the U.S., and for issuing legal notices and non-compliance with regulations. In addition, the information will be used for trend analysis and agricultural risk assessment support.
- Providing information regarding the effectiveness of AQI and the association of pests with the cargo, mail, and passenger pathway.
- Supporting operational and policy planning and decision-making for delivering efficient, effective and responsive programs, safeguarding American agriculture, and facilitating safe trade.

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.

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

Open-source port, airport, and taxonomy lists are used to align system data with external unique identifiers.

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 information. Role-based security includes the use of USDA e-Authentication services, which provides user authentication. User roles are granted through web-of-trust mechanismsin place.

SSL encryption is used to protect data being transferred over the wire. System credentials which support 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?

The records are permanent 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.

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 information. Role-based security includes the use of USDA e-Authentication services, which provides user authentication. User roles are granted through web-of-trust mechanism in place.

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 with all organizational units and programs within PPQ. Information shall be utilized in support of all aspects of the PPQ mission and in support of activities associated with protecting U.S Agriculture and natural resources. Information may be shared with APHIS and AMS organizational units and programs (outside of PPQ) on a need-to-know basis consistent with, and to support their mission.

4.2 How is the information transmitted or disclosed?

Information is transmitted electronically via email or directly through the database interface as well as through verbal communications between program officials. Sharing information internally is decided on a case-by-case basis, consistent with mission objectives. Program personnel use this information for pathway analysis, trade, risk analysis, science, and any other uses necessary to carry out the mission of the agency and program.

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 protected based on information within the network is encrypted during transmission and is only sent to personnel with a need-to-know in accordance with ARM processes. Data in the system is accessible to authorized ARM 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 are determined and controlled by user roles and an access matrix that is controlled by PPQ management.

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 e-Authentication services, which provides user authentication. User roles are granted through web of trust mechanisms in place.

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?

Data is shared with DHS CBP. CBP inputs inspection results, communicates the results to USDA and prepares non-compliance notifications. Reports and trends are shared with CBP for staffing purposes and to allow for DHS to make risk-based decisions about the admissibility of commodities imported into the U.S.

Reports are also shared with State and foreign entities to inform them of upcoming plant shipments and/or noncompliant shipments destined to their State or originating from their country.

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. Sharing of personally identifiable information (PII) outside the Department is compatible with the original authorities and reasons for data collection only if the sharing of such data is associated with Departments and Agencies who share or act on behalf of USDA APHIS regulatory and legal authorities. These includeThe Plant Protection Act, 7 U.S.C. § 7701-7772 and 7 U.S.C. § 7781-7786; Honey Bee Act, 7 U.S.C. § 281-286; and The Animal Health Protection Act, 7 U.S.C. §8301-8321.
The SORN coverage for ARM currently is Agricultural Quarantine Activity System (AQAS), USDA/APHIS–20 since the ARM SORN is in the process of being published

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

The information shared electronically with CBP has the following security measures for safeguarding transmissions. The information exchange is encrypted using FIPS 140-2;AES-256 encryption algorithms over the DHS Extranet configured with IPSEC encrypted tunnels. Additional information is shared with users pulling reports. Only authorized users have access to the system and they have to use eAuthentication to access the system. They all receive security

awareness training which informs them on how to handle information. Not all data will be accessible by any user; functionality and access will be determined and controlled by user roles.

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

There is a risk of data being transmitted externally and the risk is mitigated based on the fact that the data that is exchanged is encrypted using FIPS 140-2;AES-256 encryption algorithms over the DHS Extranet configured with IPSEC encrypted tunnels. There is also a risk of unauthorized access to the data in the system, but it is only accessible to authorized ARM 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 will be determined and controlled by user roles and an access matrix that is controlled by PPQ management.

Likewise, DHS Customs and Border Protection (CBP) inspectors will also have access to the data in this system. Access will be controlled in the same way as for USDA users; through eAuth accounts and ARM System user roles applied to an access matrix.

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 e-Authentication services, which provides user authentication. User roles are granted through web of trust mechanisms in place.

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.

A SORN is required and is in the process of being published. Until then, notice is provided through the publication of this PIA on the Internet.

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

No.

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

Generally, the decision to enter into the U.S. or import goods/merchandise or receive foreign mail packages into the United States is within the discretion of the individual or company. However, United States law requires persons seeking to enter the US or to import regulated items to provide sufficient information to allow USDA APHIS to determine whether the individual poses a risk or to determine whether the imported goods/merchandise pose an agriculture or natural resource risk to the country. If the individual or company does not provide the required information then they cannot meet the regulatory requirements for imported products, foreign mail, and travel to the US.

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

Because the submission of information is required for persons seeking to enter the US or the import of regulated items or foreign mail, restrictions on APHIS use and sharing of information is limited to the legal requirements set forth in the Privacy Act, Trade secrets Act, and the uses of published System of Records Notifications (SORN). Individuals or companies do not have the right to consent to the particular use of the information collected in ARM. If the individual or company does not provide the required information then they cannot meet the regulatory requirements for imported products, foreign mail, and travel to the US.

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.

As mentioned in 6.1 of this section, APHIS will be issuing a System of Records Notice (SORN). Notice is also provided through the USDA internet publication of this PIA. Additionally, USDA has set up a web site to provide an additional opportunity to view published PIA's and SORN's https://www.usda.gov/privacy-policy.

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.

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

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

They are not notified as ARM is not publicly accessible and individuals would need to follow the procedures listed in 7.1 and the PIA which is publicly available on the USDA website https://www.usda.gov/privacy-policy.

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 risk associated with the redress available. The redress procedures were developed based on the requirements of the Privacy Act.

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?

Initial requests for grants to the system are routed from the user through their supervisor to the system owner. Need-to-know determinations are made at both the supervisor and system owner level. If validated, the request is passed on to the ARM Help Desk. The user and system owner are notified via email that the request has been processed along with instructions for the initial login. User profile modification requests follow the same process as for an initial request. If an individual has not used the system for more than 90 days, that individual's access will be denied, and the same procedures as noted above must be completed to renew access. This process is documented in the "ARM Application and Datamart Access and Reporting Guidance" document.

8.2 Will Department contractors have access to the system?

Yes, subject to the same background, training, need-to-know and confidentiality requirements as employees.

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 complete annual Information Security Awareness Training. The records are stored electronically for verification purposes. If an individual does not take training, he/she will lose access. 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?

Authority to Operate was granted on 9/16/2021.

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

ARM utilizes robust authentication and authorization via USDA e-

Authentication and Physical access control, firewalls (access control), and intrusion detection systems prevent unauthorized access and misuse of data. ARM utilizes audit trails to track data inserts and edits for all major data elements and tables within the system. Below is user system activity that is audited and is maintained for three years:

- Records created or modified associated with inspections
- User interactions in a workflow

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 ARM 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 which detail objects accessed by users. Role-based access controls are enabled to provide least privilege. Secure Socket Layer (SSL) is used to protect data being transferred over the wire. System credentials which support system access control are protected using strong one-way hash. Passwords are obscured while users input their credentials to access the system.

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?

ARM is a web-based application that supports the operational and analytical needs of USDA APHIS PPQ and the Department of Homeland Security (DHS) Bureau of Customs and Border Protection (CBP) Agricultural Quarantine Inspection (AQI) programs.

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

No, integrity, privacy, and security are reviewed in accordance with APHIS IT security and privacy policy and are reflective of the successful transition throughcertification and accreditation, and investment management processes.

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?

There is no use of 3rd 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

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.