Privacy Impact Assessment
AGRICULTURAL RISK MANAGEMENT (ARM)

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

Privacy Impact Assessment for the

AGRICULTURAL RISK MANAGEMENT (ARM)

August 3, 2018

Contact Point
Nancy D. Matthews
USDA APHIS
301-851-2059

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

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

Abstract

The Agricultural Risk Management (/\RM) System is a Web-based. Service-oriented system that will support 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. It will also support the diagnostic and regulatory action needs of Federal and State domestic activities and Smuggling Interdiction and Trade Compliance (SlTC) activities focused on mitigating the risks associated with invasive species. The ARM System will replace the existing PPQ IT systems (in particular the Agricultural Quarantine Activity Systems {AQAS). The PIA is being conducted because the system will be collecting information from the public that is personally identifiable.

Overview

The ARM System will support the capabilities for tracking, management and handling of inspections of agricultural imports into the United States. 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, Regulatory Action, and System Support. In support of the related USDA processes, The ARM System collects data resulting from the inspection of shipments and personnel at U.S. Ports of Entry. This information is collected primarily by Customs and Border Protection (CBP) officers and USDA PPQ inspectors. CBP conducts inspections at ports of entry, to include sea, air, and land border crossings. PPQ inspectors accomplish inspections at various Plant Inspection Stations around the country. Inspection data includes information about the inspection location, shipper, origin and destination of the shipment, the shipment mode of transportation, commodity data, and inspected persons data. 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.).

Domestic diagnostic requests come from USDA Smuggling Interdiction and Trade Compliance (SITC) inspections where pests are intercepted from within the U.S. and passed to ARM for identification support.

Where violations are determined, notifications will be prepared and sent to permit holders, importers, or brokers. 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.

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?

- Business location and address information
- Business Point of Contact Name
- Shipment and commodity information 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 customs 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 data collected from inspection worksheets
- Pest diagnostic data input and treatment recommendations made by USDA employees
- Taxonomic data imported from ITIS (one-time import)
- Commodity data collected from shipment documents and invoices provided by shippers

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

- Collect, communicate, and analyze inspection data for shipments. conveyances, and
- personnel arriving in the U.S.
- Issuing legal notices and non-compliance with regulations

1.4 How is the information collected?

Information is collected electronically by ARM. Brokers use the Automated Broker Interface (ABI) to enter shipment information which is then sent to the CBP Automated Commercial Environment (ACE). CBP Agricultural Specialists input inspection information from shipment bills of laden or invoices into ACE and this information is electronically transferred to ARM.

1.5 How will the information be checked for accuracy?

Address data will be verified through comparison to addresses previously entered data in ARM. Data collected from user supplied data will be scrutinized by CBP officers and USDA inspectors. Organizational names will be compared to existing data in ARM.

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; and the Animal Health Protection Act, 7 U.S.C. §8301-8321. POAM 21572 has been created to address the SORN deficiency.

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

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.

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.

- 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 to make recommendations regarding the type of treatment that may be required.
- Taxonomic data is used to collect, communicate, and analyze inspection data for shipments, 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.

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.

Commercial or publically available shipping data is used 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.

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 mechanisms in 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.

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?

APHIS will maintain records indefinitely while the records schedule is awaiting approval. This qualifier is supported under 36 CFR 120.18.

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

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

4 Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

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

N/A

4.2 How is the information transmitted or disclosed?

N/A

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.

N/A

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?

Data will be shared with DHS CBP. CBP will input inspection results and communicate the results to USDA and prepare non-compliance notifications. Reports and trends will be shared with 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.

Yes. It is not currently covered under a SORN but POAM 27762 has been created to address this deficiency. 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 include 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; and The Animal Health Protection
Act, 7 U.S.C. §8301- 8321

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

The information is shared electronically with 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.

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

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 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.

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?

APHIS will be issuing a new System of records Notice (SORN) in conjunction with this PIA. Notice is also provided through the publication of this PIA on the Internet. Additionally, USDA has set up a web site to provide an additional location to view published PIA's http://www.usdagov/wps/portal/usda/usdahome?navid=PRIVACY_POLICY_ES.

6.2 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 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.

6.3 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 regulated items, restrictions on APHIS use and sharing 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. As for the use of the information, once it is presented to APHIS in an importation or individual entry, the individual or companies no longer retain rights respecting their consent to the use of the information.

6.4 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.

As mentioned in 6.1 of this section, APHIS will be issuing a new System of Records Notice (SORN) in conjunction with this PIA. Notice is also provided through the publication of this PIA on the Internet. Additionally USDA has set up a web site to provide an additional opportunity to view published PIA's

7 Section 7.0 Access, Redress and Correction

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?

Procedures for individuals to gain access to data maintained in ARM would be covered by the respective SORN for this system. In addition, the freedom of information act (FOIA) (5U.S.C 522) provides a means of access to the information for all individuals, irrespective of the individual's status under the privacy act.
Under FOIA, certain records may be withheld in whole or in part from the requester if they fall within one of nine FOIA exemptions. Six of these exemptions most often form the basis for the withholding of information by APHIS:

- Exemption 2: Protects certain records related solely to APHIS' internal rules and practices.
- Exemption 3: Protects information that is prohibited from disclosure by other laws.
- Exemption 4: Protects trade secrets and confidential commercial or financial
- Information.
- Exemption S: Protects certain inter-agency and intra-agency communications.
- Exemption 6: Protects information about individuals in personnel, medical, and similar files when disclosure would constitute a clearly unwarranted invasion of privacy.
- Exemption 7: Protects records or information compiled for law enforcement purposes when disclosure
    a. could reasonably be expected to interfere with enforcement proceedings;
    b. would deprive a person of a right to a fair trial or an impartial adjudication;
    c. could reasonably be expected to constitute an unwarranted invasion of personal privacy:
    d. could reasonably be expected to disclose the identity of a confidential source;
    e. would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions, if such disclosure could reasonably be expected to risk circumvention of the law; or
    f. could reasonably be expected to endanger the life or physical safety of an individual.

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

Any individual who wishes to request correction or amendment of any record pertaining to him or her contained in a system of records maintained by an agency shall submit that request in writing in accordance with the instructions set forth in the system notice for that system of records. The Privacy Act requires agencies maintaining personal information about individuals to keep accurate, relevant, timely, and complete files. If individuals believe ARM contains incorrect information and should be amended, they may contact the agency directly to request a change.

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

Publication of the Systems of Records Notification (SORN) provides information on access and amending information collected in ARM. The agency also provides the public with information via publically accessible web sites.

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.

As noted in 7.1 of this section, individuals may seek access to information collected in ARM pursuant to FOIA, and as a matter of APHIS policy, redress may be requested directly from the agency.

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?

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.

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?

Authority to Operate was granted on 25 August 2015.

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, 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.

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?

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.

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?

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 through certification and accreditation, and investment management processes.

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)?

N/A

10.10 Does the system use web measurement and customization technology?

N/A

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 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