Smuggling Interdiction and Trade Compliance (SITC) National Information, Communcation and Activity System Privacy Impact Assessment

Technology, Planning, Architecture, & E-Government

- Version: 1.2
- Date: March 22, 2012
- Prepared for: USDA OCIO TPA&E

USDA

United States Department
of Agriculture

Privacy Impact Assessment
SNICAS

March 22, 2012

<u>*Contact Point*</u>
Nancy D. Mathews
APHIS/PPQ
(301) 734-0874

<u>*Reviewing Official*</u>
Tonya Woods
APHIS Privacy Officer
(301) 851-4076

Danna Mingo
Information Security Branch
(301) 851-2487

Abstract

United States Department of Agriculture (USDA), Animal Plant Health Inspections Service (APHIS), Plant protection and Quarantine (PPQ), is publishing this Privacy Impact Assessment to give notice of its procedures for recording certain information associated with its Smuggling Interdiction and Trade Compliance (SITC) program/unit. Information for the program/unit is collected in the SITC National, Information, Communication, and Activity System (SNICAS). The primary goal is to maintain information about individuals, commercial entities, and companies, who import, handle, distribute or consume products that may pose, either indirectly or directly, a smuggling or trade compliance risk to U.S. agriculture and natural resources. The secondary goal is to maintain and communicate information associated with SITC operational and administrative activities.

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

Overview

The mission of Plant Protection and Quarantine's (PPQ's) Smuggling Interdiction and Trade Compliance (SITC) Program is to detect and prevent the unlawful entry and distribution of prohibited and/or non-compliant products that may harbor exotic plant and animal pests, disease or invasive species. SITC focuses its anti-smuggling and trade compliance efforts at the Ports of Entry (POE) and in commerce to prevent the establishment of plant and animal pests and diseases, while maintaining the safety of our ecosystems and natural resources. SITC is responsible for collecting, maintaining, and reviewing information appropriate to successfully and efficiently meet this mission.

SNICAS is a Plant Protection and Quarantine Investment in the Animal and Plant Health Inspection Service portfolio. SITC collects data maintained in SNICAS pursuant to the Plant Protection Act 7 U.S.C. 7701-7786; Animal Health Protection Act 7 U.S.C 8301-8321; 7 The Honey Bee Act U.S.C. 281-286; Bioterrorism Preparedness and Response Act of 2002 (7 U.S.C. 8401)

PPQ SITC, will in most cases collect information through physical inspection and survey of POE and commerce site locations. Alternatively, where available and appropriate, PPQ SITC will leverage internal agency datasets to supplement data not obtained during physical inspections/surveys. PPQ SITC will also, where available and appropriate, obtain and record information from other outside sources including, but not limited to, federal, state, and local governments, as well as stakeholder, cooperator, and open source data sets. Electronic data transfer is the preferable method of recording and collecting data, but when necessary, SITC will manually type in data sets gleaned from other sources.

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?

SITC will collect information pertaining to individuals, commercial entities, and companies, who import, handle, distribute or consume products that may be associated with the importation and/or interstate movement of prohibited or restricted agricultural products. The system will also maintain and communicate information about SITC operational and administrative activities. Specifically, the system will contain records pertaining to the POE and commerce locations inspected/surveyed during daily operations. Information collected includes:

- Company/Business/Entity Name
- Persons Name (First, Middle and Last)
- Address, City, State, Zip code, Latitude and Longitude
- Phone, Fax, and Email
- Social Security Number (or other personal ID number)
- Date of Birth
- Gender
- Inspection/Survey Date
- Conveyance and Conveyance ID (License plate, Vehicle Identification Number)
- Tax Identification Number
- Product Name, photograph, Country of Origin, Id numbers, and Bar codes
- Port of Entry, Crossing, or Import location
- Legal Authorities, and CFR's
- Employee information, SITC work unit, and area of coverage.
- Supporting documents (attachments)

Other communicative and analytical information associated with products, seizures, trace requests, product pathways, recall activities, and intelligence/analysis background reviews in support of the SITC mission will also be collected.

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

To the extent available, this information is collected directly from individuals, commercial entities, and companies, who import, handle, distribute or consume products that may be associated with the importation and/or interstate movement of prohibited or restricted agricultural products. Where available and appropriate, PPQ SITC will leverage internal agency datasets to supplement data not obtained during physical survey/inspections. PPQ SITC will also, where available and appropriate, obtain and enter information from other outside sources including, but not limited to, federal, state, and local governments, as well as stakeholder, cooperator, and open source or commercial data sets. Data associated with operational and administrative functions will be collected directly from SITC employees (officers, supervisors, administrators and support personnel).

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

The principal purpose for collecting this data is to provide APHIS, PPQ, SITC and other agency personnel with information to assist them in detecting and preventing the unlawful entry and distribution of prohibited and/or non-compliant products that may harbor exotic plant and animal pests, diseases, or invasive species.

1.4 How is the information collected?

Information in SNICAS is primarily manually entered by SITC employees as a result of physical inspection/survey associated with daily operational deployment of the program. When collecting data from outside sources electronic data transfer is the preferable method, but when necessary, SITC will also manually enter these data sets.

1.5 How will the information be checked for accuracy?

All data is quality controlled and reviewed for accuracy at the time of entry by the SITC employee (officer, supervisor, etc.) During operational deployment employees also confirm the accuracy of the data with the individuals, commercial entities, and companies being surveyed /inspected. SNICAS was also deployed with current industry standard architecture technologies to ensure data quality and integrity. These data integrity rules assist employees when entering data. Examples of industry standard architectures deployed within SNICAS include:

- SNICAS is a relational database and makes extensive use of primary and foreign key values. These primary and foreign key relationships (constraints) are fundamental in ensuring and checking for data quality and integrity. This occurs

within the main architecture of the system, as well as, within the many reference tables deployed and utilized for drop down menus

- For each record saved in SNICAS the system as a minim amount of data that must be collect for every record to be valid. By forcing this minimum the systems (by default) have data of higher quality and integrity.

- SNICAS enforces data integrity rules on specific data elements: Including (but not limited to), dates, zip codes, county names, state names, country names, seizure quantities, work units, and officer names.

- SNICAS enforces data integrity rules based on relational data: Including (but not limited to), Officer and Work Unit, Survey Location and Work unit, Location and Survey, Trace Location and Work unit, Trace requesting and receiving unit (office), as well as, seizure articles and seizure surveys.

- SNICAS utilizes audit trails to track data edits for all major data elements and tables within the system. Virtually, this is a database behind the database and allows administrators not only to review changes within the system, but to also restore data inaccurately entered if needed.

Data is also quality controlled by the SITC analysts and SNICAS programmers on a quarterly, six-month and annual review. The location information is geo-coded for accuracy concerning latitude and longitude while violation and seizure data are cross-referenced with other PPQ databases to determine if any discrepancies occur. Individuals and commerce site locations associated with the pathways used to disseminate prohibited and regulated commodities are also cross-referenced in third party databases such as LexisNexis, Autotrack, Sales Genie and other third party sources.

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

Plant Protection Act 7 U.S.C. 7701-7786; Animal Health Protection Act 7 U.S.C 8301-8321; 7 The Honey Bee Act U.S.C. 281-286; Bioterrorism Preparedness and Response Act of 2002 (7 U.S.C. 8401)

SITC conducts activities, and investigations which is derived from APHIS regulatory authority in Title 9 of the code of federal regulations (CFR) for plants, plant products or plant pests, as well as from Title 7 of the CFR for biological toxins and agents, domestic quarantines, endangered species, foreign quarantines, genetically engineered organisms, Hawaii quarantines, honey bees, import /export, noxious weeds, plant pests and the seed act.

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.**

Integrated Network Authentication is required for access to the system. The access control list for the database validates against the network identification of the user creating a 2-layer authentication scheme. SITC personnel have access to all data in the system. Non-SITC personnel are provided data feeds or have restricted views of the database based on their database account. These accounts use integrated network authentication to validate the end user and restrict access.

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 primary goal of SNICAS is to maintain information about individuals, commercial entities, and companies, who import, handle, distribute or consume products that may pose, either indirectly or directly, a smuggling or trade compliance risk to U.S. agriculture and natural resources. The secondary goal is to maintain and communicate information about or associated with SITC operational and administrative activities.

The information in SNICAS is used in the following ways:

- To support the safe and efficient daily deployment of SITC operations.
- To support management and administration of the SITC program
- As legal documentation to support the chronological and historical chain of events associated with activities or regulatory actions taken.
- To locate prohibited commodities and identify individuals, business entities, and affiliated personnel associated with those locations that either purchased or distributed the regulated articles within U.S. commerce.
- To communicate, document, and respond to trace back and trace forward information exchanged between work units, areas, and regions.

- To help support targeting, trend, pathway, and risk analysis initiatives in support of the APHIS mission.
- To help determine the risk status of the commercial sites where the regulated articles were seized.
- To generate reports to evaluate quality control of data and effectiveness of the program for risk based decisions, staffing models, statistical analysis, work efficiency and productivity based on that data.
- To Provide data for modeling potential pest and/or disease outbreaks based on the product pathway as it correlates to the country of origin's pest and/or disease status
- To support the regulatory actions, investigations, and cases generated by the APHIS, and the SITC program.
- Shared, when appropriate, with other agencies, units, and state departments of agriculture to support their regulatory actions, investigations, and cases.

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

N/A

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

Open source publically available data, as well as LexisNexis, Autotrack, Sales Genie, DUNS and Bradstreet, and other commercial available data is used by SITC as supplemental and confirmatory information to support data obtained during physical inspections/surveys. Open source and commercially available data is also utilized by SITC for background information and analysis. Information is leveraged to identify potential violators or affiliations or associations with known violators.

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.

Integrated Network Authentication is required for access to the system. The access control list for the database validates against the network identification of the user creating a 2-layer authentication scheme. SITC personnel have access to all data in the system. Non-SITC personnel are provided data feeds or have restricted views of the database based on their database account. These accounts use integrated network authentication to validate the end user and restrict access.

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 data will be 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 the data is retained. Data continues to inherit all security features mentioned in section 2.4 of this document. Individuals and organizations who intend to smuggle pose a grave risk to U.S Agriculture and natural resources. They employ a variety of means to establish associations and contacts for the purpose of facilitating illegal movement of products. Under these conditions, data is not purged from the system because entities, individuals, companies, corporations etc., recorded in the system have an infinite or indeterminate longevity to pose a risk to U.S Agriculture or natural resources. Data is not purged from the system because violator history can impact future enforcement actions. This retention period is consistent with APHIS legal authorities and the SITC mission.

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 maintained in SNICAS may be 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 organizational units and programs (outside of PPQ) on a need to know basis consistent with, and to support their mission.

Currently data is shared routinely within PPQ in support of specific activities associated with its mission. Currently data is also shared routinely with APHIS Investigative Enforcement Service (IES) on a need to know basis and in conjunction with investigation, violations and cases they prosecute on behalf of the PPQ SITC program/unit.

4.2   How is the information transmitted or disclosed?

Information is transmitted electronically via email or directly through the database interface and via an external reporting site, as well as through verbal communications between program officials. Sharing information within APHIS is decided on a case by case basis, consistent with mission objectives. APHIS 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.

SNICAS has built in granularity based on what level of access the National Coordinator deems as an appropriate level of access to APHIS employees. This level of access is based on their needs without compromising the integrity or security of the data. When appropriate and prudent, SITC personnel will redact any personally identifiable information from shared reports.

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?

Ad hoc limited information sharing with external agencies and departments (outside of APHIS) will require an official request directly to the Plant Health Programs (PHP) executive within PPQ, where SITC resides. Long term exchanges of data from external agencies and departments will require a Memorandum of Understanding (MOU) that outlines third party sharing, privacy, and data security requirements.

Currently data is also shared routinely with Department of Homeland Security (DHS) Customs and Border Protection (CBP) on a need to know basis and in conjunction with their cooperative mission to protect US Agriculture and natural resources during inspections conducted, on behalf of USDA, at our nation's borders and Ports of Entry (POE). This information sharing provides CBP with the necessary targeting and background information to accomplish this mission and may contain identifying information such as an individual's name, address, and importer identification number.

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.

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. 7701-7786; Animal Health Protection Act 7 U.S.C 8301-8321; 7 The Honey Bee Act U.S.C. 281-286; Bioterrorism Preparedness and Response Act of 2002 (7 U.S.C. 8401) and is derived from APHIS regulatory authority in Title 9 of the code of federal regulations (CFR) for plants, plant products or plant pests, as well as from Title 7 of the CFR for biological toxins and agents, domestic quarantines, endangered species, foreign quarantines, genetically engineered organisms, Hawaii quarantines, honey bees, import /export, noxious weeds, plant pests and the seed act.

If data is shared with Departments or Agencies who do not act on behalf of USDA APHIS regulatory and legal authorities then PII is not shared unless both Departments and Agencies have signed a Memorandum of Understanding (MOU) that assures protection of all PII data.

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

Information is transmitted electronically via email or directly through the database interface and via an external reporting site, as well as through verbal communications between program officials. Sharing information outside of APHIS is decided on a case by case basis, consistent with mission objectives.

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

When sharing information with third parties, the same specifications related to security and privacy that are in place for USDA APHIS employees are also applied to these outside Departments or Agencies. Access to SITC data is governed by the "need to know" criteria and requires that the receiving entity demonstrate the need for the data before access or interface is granted. The reason for the exchange/interface request and the implications on privacy are two factors included in both the initial and ongoing authorization, the MOU, and the Interconnectivity Security Agreement (ISA) negotiated between APHIS PPQ and the external agency seeking to access to APHIS PPQ SITC data. In general terms the MOU specifies the conditions that govern the limitations associated with the use of the data, while the ISA specifies the data elements, format and the interface utilized during an electronic exchange.

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.usda.gov/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 whether to import goods/merchandise into the United States or to transport those goods across state lines is within the discretion of the individual or company. However United States law requires persons seeking the importation or interstate movement of regulated items are required to provide sufficient information to allow USDA APHIS to determine whether the 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 the importation or interstate movement of goods/merchandise, 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 SNICAS. As for the use of the information, once it is presented to APHIS in an importation or interstate movement context, the individual or companies no longer retain rights respecting their consent to the use of the 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.

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

http://www.usda.gov/wps/portal/usda/usdahome?navid=PRIVACY_POLICY_ES

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 SNICAS 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 5: Protects certain interagency 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 SNICAS 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 SNICAS. The agency also provides the public with information via publically accessible we sites. For example the FOIA Reading Room can be accessed at the following we address:

http://www.aphis.usda.gov/foia/foia_reading_room.shtml

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 SNICAS pursuant to FOIA, and as a matter of APHIS policy, redress may be requested directly from the agency.

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?

All user groups including SITC employees have access to the system defined by specific user's profile and limited through the rights and responsibilities of each user. Access by Users, Manager, Systems Administrators, Developers, and others is defined by access levels associated with the mission and/or operating functions. User access is based on a demonstrated need-to-know basis.

8.2   Will Department contractors have access to the system?

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

8.3   Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All APHIS personnel are required to complete the Computer Security and Accessibility test annually

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

The system is currently undergoing C&A phase I certification and accreditation.

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

SNICAS utilizes audit trails to track data edits for all major data elements and tables within the system. Virtually, this database behind the database allows administrators not only to review changes within the system, but to also restore data inaccurately entered if and when appropriate.

All data are quality controlled by the SITC analysts and SNICAS programmers on a quarterly, six month and annual review.

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?

Integrated Network Authentication is required for access to the system. The access control list for the database validates against the network identification of the user creating a 2-layer authentication scheme. SITC personnel have access to all data in the system. Non-SITC personnel are provided data feeds or have restricted views of the database based on their database account. These accounts use integrated network authentication to validate the end user and restrict access.

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?

SNICAS is a nationally utilized, moderate impact, major application. It is accessed through a web based interface and is utilized as the primary tool to record, communicate, and track program activities. SNICAS is a legacy system utilized by the SITC program/unit to collect mission appropriate data and leveraged to help deploy the program and protect U.S Agriculture and resources, on a daily basis.

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.

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"?**

N/A

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

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 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.
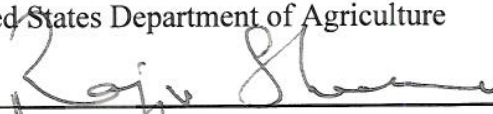
N/A

Responsible Officials

Nancy D. Matthews, PM, IT Manager
USDA, Animal and Plant Health Inspection Services (APHIS),
Plant Protection and Quarantine (PPQ)
4700 River Road
Riverdale, Maryland 20737
(301) 734-0874
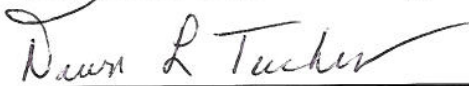Nancy D. Matthews@APHIS.usda.govUnited States Department of Agriculture

Approval Signature

Matthew Rhoads
Information System Owner
Plant Protection and Quarantine
Animal Plant and Health Inspection Service (APHIS)
United States Department of Agriculture

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

Dawn L. Tucker
Acting APHIS CIO
Animal Plant and Health Inspection Service (APHIS)
United States Department of Agriculture

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