Privacy Impact Assessment

Smuggling Interdiction and Trade Compliance (SITC) National Information, Communication and Activity System (SNICAS)

Policy, E-Government and Fair Information Practices

- Version: 1.1
- Date: January 09, 2023
- Prepared for: Marketing and Regulatory Programs (MRP)

United States Department of Agriculture

Privacy Impact Assessment for the

Smuggling Interdiction and Trade Compliance (SITC) National Information, Communication, and Activity System (SNICAS)

January 2023

Contact Point

Name	Contact Number	Email Address
Steven Schafer	970-286-5196	Steven.Schafer@usda.gov

Reviewing Official

Tonya Woods
APHIS Privacy Officer
United States Department of Agriculture
Phone: 301-851-4076
Aphisprivacy@usda.gov

Abstract

United States Department of Agriculture (USDA), Animal Plant Health Inspection 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.

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 meet this mission successfully and efficiently.

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 Honeybee 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 Port-of-Entry (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 opensource 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:

- Persons Name (First, Middle and Last)
- Address, City, State, Zip code, Latitude and Longitude (Personal and/or Business)
- Phone and Email
- Date of Birth
- Driver License
- Criminal history

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

To the extent available, this information is collected from PPQ SITC Analysts, Officers and Supervisors. 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 and SITC 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. Information is leveraged to identify potential violators,
affiliations, or associations with known violators.

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. SITC will also manually enter data information collected from interviews with individuals, paper or electronic records and visual searches (internet, signs, etc.).

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:

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. 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, CLEAR, Whooster, and other third-party sources.

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

The Plant Protection Act 7 U.S.C. 7701-7786; Animal Health Protection Act 7 U.S.C 8301-8321; 7 The Honeybee Act U.S.C. 281-286 provide SNICAS the authority to collect PII.

SITC conducts survey, inspection, trace work, seizure, destruction, and investigations 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, honeybees, import /export, noxious weeds, plant pests and the seed act.

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. Auditing of user access is performed quarterly to ensure users still need access to SNICAS.

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.
- To share data, 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?

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 publicly available data, as well as LexisNexis, CLEAR, Sales Genie, Whooster, and other commercially 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 are also utilized by SITC for background information and analysis. Information is leveraged to identify potential violators, 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.

The system implements various security concepts in order to ensure that information is handled appropriately. This includes, but is not limited to, the concept of least privilege, separation of duties, and Rules of Behavior requirements. The system complies with NIST 800-53 controls requirements. This includes controls covering access control, risk management, audit and accountability, awareness and training, contingency planning, identification and authentication, system and information integrity, incident response, maintenance, media protection and more. The system

security complies with USDA requirements to ensure that information is handled appropriately.

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 is working on the development record retention schedules, but until they are approved by NARA, electronic systems are classified as permanent in accordance with unscheduled records management policy.

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

No.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The data within SNICAS is considered permanent at this time and the access to data is restricted by strong access control methods including PIV card integration and integration with USDA's ICAM. Access to system is controlled via role-based access control which will enforce separation of duties and limit access to the data while providing adequate access to the system components for administrative purposes. The data will be encrypted at all the time whether in motion or at rest. Auditing of user accounts are completed also which ensures only appropriate personnel have access to the data.

Section 4.0 Internal Sharing and Disclosure

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

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

Currently PII data is 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.

Location data is shared with GIS to create maps for presentations, mobile app use via the GIS entry and for planning work.

4.2 How is the information transmitted or disclosed?

Information sharing between SITC staff is done via automated emails, traces and verbal communication. Automated emails are sent to CBP to share information, but there is no access to SNICAS within the emails and they can't access SNICAS. Automated reports are created and shared via a SQL database to APHIS staff outside of SITC. Any other form of information sharing would be done via Excel spreadsheets encrypted and have any PII removed. 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.

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 SNICAS processes. Data in the system is accessible to authorized SNICAS 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 is determined and controlled by user roles.

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.

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 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) with DHS CBP 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. This sharing is covered by the USDA/APHIS-21, Smuggling Interdiction and Trade Compliance (SITC) National Information Communication Activity System (SNICAS) SORN.

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 through verbal communications between program officials. Sharing information outside of APHIS is decided on a case-by-case basis, consistent with mission objectives. Email is encrypted as it is sent to CBP personnel and only sent to

personnel with a need-to-know. Data is encrypted during transit over the intranet utilizing https as it is accessed internally only. The need to know is based off the fact that a request is sent to CBP personnel when there is a target of interest that needs to be tracked on incoming shipments whether it be through air, land or sea.

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

SNICAS cannot be used to share information directly with any external agencies/organizations. SITC personnel, only, can extract the data and create reports, mitigating the risk associated with the potential unapproved access to, or release of, SNICAS data. When sharing information with DHS CBP, 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.

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.

Yes. Notice is provided through the USDA/APHIS-21, Smuggling Interdiction and Trade Compliance (SITC) National Information Communication Activity System (SNICAS) SORN.

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

Notice is provided through the USDA/APHIS-21, Smuggling Interdiction and Trade Compliance (SITC) National Information Communication Activity System (SNICAS) SORN.

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

No. 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. If this information is not provided, the individual will not be allowed to import or transport their goods within the United States.

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

No, the information is required for the importation or interstate movement of goods/merchandise within the United States.

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 new System of Records Notice (SORN) in conjunction with this PIA. 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?

The procedures are available in Section 7.1 of this document, which is publicly available on the USDA website.

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.

There are no privacy risks because redress is done according to guidelines set forth by the Privacy Act Staff.

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 access to the system are routed from the supervisor to the Business System Manager (BSM) who approves the request. Need-to-know determinations are made at the BSM level. If validated, the request is created by the system administrator. The user is 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 disabled, and the same procedures as noted above must be completed to renew access. It is not documented as this system is only accessed by SITC personnel and so, the process is known within the program.

8.2 Will Department contractors have access to the system?

No contractors will have access to the system.

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 and PII training.

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

Yes. The system's Authority to Operate expires on September 30, 2024.

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

User identification is conducted through the USDA ICAM Shared Services (e-Authentication) system and the use of specific and restrictive user roles within the system ensure only authorized personnel have access to the data within SNICAS. Physical access control, firewalls (access control), and intrusion detection systems prevent unauthorized access and misuse of data.

8.6 <u>Privacy Impact Analysis</u>: 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 identified is unauthorized sharing and mishandling of data that is shared. SNICAS is only accessed internally, and all internal users must utilize their PIV cards and e-Authentication to access the system which prevents the access of

unauthorized users to SNICAS. Data is encrypted during transmission and at rest. Auditing is enabled to track which data users have accessed. Role-based access prevents users from accessing data they are not allowed to 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 an application accessed through a web-based interface and is utilized as the primary tool to record, communicate, and track program activities.

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

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

SNICAS does not utilize 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.