

Privacy Impact Assessment NSF Center for Integrated Pest Management

Technology, Planning, Architecture, & E-Government

- Version: 1.2
- Date: September 7, 2013
- Prepared for: USDA OCIO TPA&E



Privacy Impact Assessment for the NSF Center for Integrated Pest Management

September 7, 2103

Contact Point
Deitra Phillips
APHIS/PPQ/BISSM
301-851-2307

Reviewing Official

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

Danna Mingo, APHIS Privacy Liaison
United States Department of Agriculture
(301) 851-2487

Chief Privacy Office
Office of Chief Information Office
United States Department of Agriculture

Abstract

The Center for Integrated Pest Management information system (CIPM) provides a distributed web-based system for storage, tracking, and reporting of invasive species data and data collected from quarantine treatments. The PIA is being conducted to describe the Personally Identifiable Information (PII) being captured by CIPM, how it is used and the security controls in place to protect the PII commensurate with identified risk.

Overview

The Center for Integrated Pest Management information system (CIPM) provides a distributed web-based system for storage, tracking, and reporting of invasive species data and data collected from quarantine treatments. The CIPM system facilitates those tasks involved in identifying pre-emergent invasive pests and the methods used to exclude them in addition to recording commodity treatments for imported and exported trade goods. All four of the subsystems of the CIPM information system are web-based application systems and databases developed by CIPM for a wide variety of clients

1. Commodity Treatment Information System (CTIS)

The CTIS system consists of four major applications that track quarantine activities of the USDA PPQ CPHST Treatment and Quality Assurance Unit. CTIS systems track treatment s and analyze treatment data to determine if commodities have met import/export treatment protocols.

556 Electronic Monitoring: a web-based application to track the cold-treatment of commodities imported into the United States.

Cold Treatment Online Search: an online database providing searchable records for all ships and containers certified for cold treatment.

Online 429 Fumigation Database: collects information from pre-clearance fumigations using Methyl Bromide conducted at ports of entry/export.

Treatment Manual Index Database: provides users of the PPQ Treatment Manual with an online searchable index of the treatment schedules.

2. Exotic Pest Information System (EPI)

The CTIS system consists of four major applications that track quarantine activities of the USDA PPQ CPHST Treatment and Quality Assurance Unit. CTIS systems track treatment s and analyze treatment data to determine if commodities have met import/export treatment protocols.

Global Pest and Disease Database: an archival database of invasive pest information concerning species not present in or having limited distribution in the US.

New Pest Advisory Group: a web-enabled system to track, monitor and provide recommendations to PPQ officials on new pests that are intercepted or discovered within the US .

Phytosanitary Alert System: the official web site for the US that provides International Plant Pest Committee reports on invasive species issues occurring within the US.

CAPS Pest Prioritization Questionnaire: a web-based questionnaire and summary application for the Cooperative Agricultural Pest Survey group.

3. PestLens

This system collects and databases open-source information about exotic pests and sends out a weekly report to subscribers via email.

4. Offshore Pest Information System (OPIS)

OPIS is a web-based system designed to collect, analyze and archive information about pest outbreaks and issues that occur outside of the borders of the US.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The CIPM information system (1) collects, manages and reports on commodity treatment information entered by foreign and domestic cooperators and APHIS Plant Protection and Quarantine (PPQ) employees at foreign and domestic ports of lading and entry, (2) collects and manages information about pests that are not currently present or have limited distribution in the US, (3) collects offshore information about exotic pests of concern, and (4) collects high-value information from publically available sources about pests of concern to the USDA. The data collect by this system includes bills of lading, ship and vessel information, commodity treatment protocols, treatment data, summary treatment statistics, information on the taxonomy and biology of invasive

pests, and offshore and open source information of pests of economic concern to the US.

The CIPM information system collects the following information:

- Other Data: Commodities being imported, treatment protocols, treatment data, pest data and information, open-source and scientific publications
- End-User Data: Shipper information at the port of lading (owner/consignee), first and last name, affiliation, address and email of application users and subscribers.
- Employee Data: First and last names, email and physical addresses of APHIS employees

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

Source data are provided by public subscribers to non-proprietary information (PestLens), State and University cooperators, APHIS-Plant Protection and Quarantine (PPQ) employees and authorized system users.

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

For the CTIS system, the main purpose for the information collected is to ensure that commodity treatment protocols are being applied per USDA guidelines in order to prevent the unwanted introduction of invasive pests. EPI data expedite the assessment of risk to exotic pests and help to facilitate commodity trade to foreign partners. OPIS and PestLens data are used as an early warning system to alert end-users of pest issues that are occurring offshore.

1.4 How is the information collected?

For the CTIS system, trusted foreign cooperators and authorized APHIS employees manually enter data into this system. For EPI, PestLens and OPIS, trusted University and State cooperators and authorized APHIS employees manually enter data into these systems.

1.5 How will the information be checked for accuracy?

For the CTIS System, data are collected immediately after or during treatment in real-time. APHIS port officials review data and summary reports to assess data accuracy. For PestLens and OPIS, PPQ and DHS staff review reports to ensure the data is accurate and of relevance to the PPQ safeguarding mission.

Data collected for EPI are reviewed by CPHST Risk Analysts for accuracy and applicability to risk assessment activities. All CIPM information systems provide a mechanism for system users to provide feedback and correction to the data.

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

PUBLIC LAW 106-224 (AGRICULTURE RISK PROTECTION ACT OF 2000) and numerous cooperative agreements between NCSU (CIPM) and APHIS-PPQ.

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

The CIPM PestLens system collects first and last name and an email address from public individuals that sign up for their weekly newsletter. Data subject to privacy regulations are collected from trusted and vetted foreign, state and University cooperators, so the privacy risks are limited to this group and to authorized government employees. Trusted users of the CIPM information system log into each application using login/password authentication. All connections are funneled through a secure socket layer protocol. RSA(1024 bits) and passwords are hashed using SHA-512. Passwords are hashed at the time of creation. Passwords are stored and transferred as encrypted, hashed values. Passwords are obscured when users enter their login credentials when gaining access to each system.

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.

Data are used to assess the risk of importing commodities into the US. The CTIS data is used to determine if import commodities met USDA treatment protocols in order to prevent the importation of invasive pests from other countries. EPI data is used by APHIS risk assessors and others to access invasive pest risks and to assist in developing risk mitigation strategies. PestLens and OPIS are early warning and tracking systems used by APHIS,

DHS, State and University cooperators to identify pre-emergent invasive pests before they become an issue in the US.

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

Each CIPM information system sub-system uses custom reporting and analysis tools. These reports typically do not contain privacy data.

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

The CTIS system uses publically and/or commercially available ship, container and treatment facility information to identify ships and certified containers and pre/post-treatment facilities. PestLens and OPIS use publically available information (new reports, internet articles, scholarly publications, etc) in their reports. The EPI system collects information on invasive pests from a number of databases and information systems. This information is used in pest-risk assessments.

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.

All connections are funneled through a secure socket layer protocol. RSA(1024 bits) and passwords are hashed using SHA-512. Passwords are hashed at the time of creation. Passwords are stored and transferred as encrypted, hashed values. Passwords are obscured when users enter their login credentials when gaining access to each 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?

CIPM information system is 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.

The risk associated with retaining information indefinitely is minimal. All data are backed up and stored off-site in a secure data retention facility.

Section 4.0 Internal Sharing and Disclosure

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

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

If information on a possible invasive pest affects animal hosts, then this information may be shared with USDA Veterinary Service or Wildlife Services.

4.2 How is the information transmitted or disclosed?

This information would be forwarded to the appropriate party via encrypted email.

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.

It has been determined that there are no privacy risks associated with sharing information the Veterinary or Wildlife Services.

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?

Information concerned with invasive species is shared with authorized federal agencies (DHS), State and University cooperators for the purpose of providing background information about potential pests.

- 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.**

Personally Identifiable Information (PII) is not being shared with any outside organizations.

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

N/A

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

N/A

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?**

Users of each CIPM information system application are notified of the scope of the information collected during the account creation process. Notification is also provided when the login credentials are distributed to the user.

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

No, the information collected is the necessary in order to set up the end-user account so that the user can receive their login information and access the specific application.

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

Based on end user usage and responsibilities, the APHIS project manager assigns specific roles and rights to each end user prior to the distribution of login credentials.

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.

Data privacy notice is provided to the end-user prior to application registration. APHIS project managers vet end users and assign roles and rights. Passwords are hashed and encrypted during transmission and storage. This serves to minimize and mitigate data privacy risks.

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?

One of two account creation methods is employed.

- (1) For some application, the APHIS project manager requests account creation information from a end-user requesting login credentials. The project manager enters this information and a system-generated email is sent to the user with their login credentials. The initial login credentials contain a temporary password which must be changed the first time the end-user accesses the system.
- (2) In other applications, an account request page is accessible. The requestor enters the required information. End users with a valid government email address are automatically added to the system. Other requests are forwarded to the APHIS project manager to review and approve or reject. End-users are sent a system-generated email containing their login credentials. The initial login credentials contain a temporary password which must be changed the first time the end-user accesses the system.

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

One of three account methods is employed to correct or modify end-user account information.

- (1) For some application, the end-user emails the APHIS project manager their modification request. The project manager modifies the information and a system-generated email is sent to the user with their updated information. If a password reset is requested, the temporary password supplied must be changed the next time the end-user accesses the system.
- (2) In other applications, an account modification page is accessible. The end-user accesses the system application and navigates to the personal information modification page. If the end-users modify their login ID or password, once this information is saved, they are logged out of the system and must login again with their new login credentials.
- (3) If an end user forgets their login ID or password, they can access a login-credential reset form by entering their valid email address registered in the application system. Once the request is submitted, a system-generated email is sent to the user with their updated information. If a password reset is requested, the temporary password supplied must be changed the next time the end-user accesses the system.

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

After account generation, end-users receive an email containing their login credentials. This email also contains information for the procedures used to correct or modify their account information. Also, this information is available to end-users once they log into each system on the user account administrative section web page.

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

N/A

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

The methods employed to address the approval process risk effectively mitigates these risks. Thus, privacy risks are minimal.

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?

One of two account creation methods is employed.

- (1) For some application, the APHIS project manager requests account creation information from a end-user requesting login credentials. The project manager enters this information and a system-generated email is sent to the user with their login credentials. The initial login credentials contain a temporary password which must be changed the first time the end-user accesses the system.
- (2) In other applications, an account request page is accessible. The requestor enters the required information. End users with a valid government email address are automatically added to the system. Other requests are forwarded to the APHIS project manager to review and approve or reject. End-users are sent a system-generated email containing their login credentials. The initial login credentials contain a temporary password which must be changed the first time the end-user accesses the system.

User login credentials are stored in the application database.

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?

Users of the CIPM information system are required to take privacy and cyber security assessments annually. These records are stored in CSAM as part of the SA&A certification.

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

No

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

The CIPM information system generates audit records for the following events: account logon events, account management events and privilege use failures. All end-user accounts are created using role-based access levels specified by the APHIS project manager. All connections are funneled through a secure socket layer protocol (SSL) using RSA (1024 bits) encryption. All system passwords are hashed using SHA-512. Passwords are to be 9 to 12 characters long, contain at least one uppercase letter, contain at least one lowercase letter and contain one non-alphabetical character, which includes numbers and/or these special characters: (e/g/, ! # \$ % = + : ; , ? ~ * -).

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 CIPM information system has implemented security controls based on NIST Special Publication 800-53 - Revision 3 security control requirements. Implementation of this control set adequately mitigates risk and has been approved by APHIS-PPQ.

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?

All applications hosted within the NSF Center for Integrated Pest Management Information System are web-based applications on a standard technology platform and are Categorized as Low.

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?

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

If so, is it done automatically?

N/A

If so, is it done on a recurring basis?

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

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

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

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

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

Responsible Officials

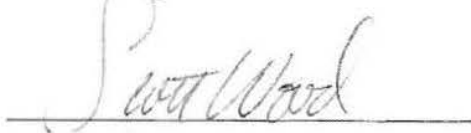
Deitra Phillips

APHIS/PPQ/BISSM

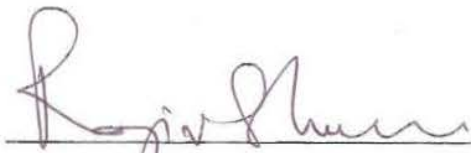
United States Department of Agriculture



Approval Signatures



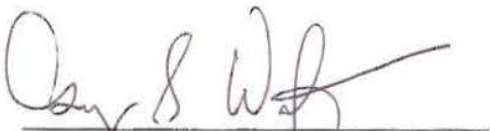
System Owner
Animal and Plant Health Inspection Service
United States Department of Agriculture



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



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



Gary Washington, APHIS CIO
Animal and Plant Health Inspection Service
United States Department of Agriculture