Privacy Impact Assessment
PLANTS

Technology, Planning, Architecture, & E-Government

- Version: 1.01
- Date: July 31, 2013
- Prepared for: USDA OCIO TPA&E

USDA

United States Department of Agriculture

Privacy Impact Assessment for the

PLANTS

31 July 2013

Contact Point
Roel Vining
Natural Resources Conservation Service
970-295-5375

Reviewing Official
Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture
202-720-8493

Abstract

The PLANTS application is a system of the Natural Resources Conservation Service (NRCS).

The Plants Database System is made available to the general public through the PLANTS web application, which provides standardized information about the vascular plants, mosses, liverworts, hornworts, and lichens of the U.S. and its territories.

A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the Federal Information Security Management Act of 2002 (FISMA) and the E-Government Act of 2002 (Public Law. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) Federal Law.

Overview

The PLANTS application is a system of the Natural Resources Conservation Service (NRCS).

The purpose of PLANTS is to provide standardized information to the general public regarding the vascular plants, mosses, liverworts, hornworts, and lichens of the U.S. and its territories. This information primarily promotes land conservation in the United States and its territories, but academic, educational, and general use is also encouraged. The PLANTS application reduces government spending by minimizing duplication and making information exchange possible across agencies and disciplines.

The PLANTS application does not directly "collect" any PII from any individual. The Plants Database System primarily maintains non-PII such as plant names, plant symbols, checklists, distributional data, species abstracts, characteristics, images, crop information, automated tools, onward Web links, and references. The public PII that is maintained in the PLANTS application database includes the names and typical contact information for individuals that hold copyrights for the photographs of plants that are displayed by the PLANTS application.

no street addresses— only email addresses.

While the PLANTS application does not have any transaction functionality related to PII, it does provide the capability for public users to:

- See a list of the plants in their state.
- Learn about the wetland plants in their region.
- Learn about all the endangered plants of the U.S.
- Learn about noxious and invasive plants.
- Search for and view images of plants.
- Read and print abstracts about important conservation plants.
- Download data or posters.
- Choose plants for particular land conservation purposes.
- Obtain general information (FAQ, Help, Contact Us, etc.).

Authority to operate PLANTS was previously provided via the ATO granted in 2010.

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?

- No PII is directly collected from any individual by this application.
- The PII that is maintained by PLANTS includes the names and typical contact information for individuals that hold copyrights for the photographs of plants that are displayed by the PLANTS application.
- To preserve the rights of the copyright holders, PLANTS is required to freely disseminate the public PII information that is maintained within PLANTS. The PLANTS application does not make any other use of this public PII.

filtered through authorized personnel

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

- No PII is directly collected from any individual by this application.
- The PLANTS application does not allow direct input of any PII from any individual (including copyright holders), because the PLANTS web application does not have any user interface (UI) that would allow for any input of any PII.
- Photographs and related information (including the PII related to the copyright holder for the photographs) are collected, managed and periodically released by processes that are outside of the accreditation boundary of this application.

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

- No PII is directly collected from any individual by this application.
- To preserve the rights of the copyright holders, PLANTS is required to freely disseminate the public PII information that is maintained within PLANTS. The PLANTS application does not make any other use of this public PII.

1.4 How is the information collected?

- No PII is directly collected from any individual by this application, nor is PII collected from any other third party sources.

1.5 How will the information be checked for accuracy?

- The accuracy of information related to the photographs (including the PII related to the copyright holder for the photographs) is checked by processes that are outside of the accreditation boundary of this application. This information is reviewed for accuracy and is verified through manual review and comparison with existing agency data. This is done by NRCS personnel who have the requisite knowledge and responsibility for the data.

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

While PLANTS does not directly "collect" any PII from any individual, these pertain:

- Federal Register /Vol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)

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

- PLANTS does not directly "collect" any PII from any affected individual.
- No privacy risks are associated with the public PII that is maintained for the copyright holders within the application. The PLANTS application is required to freely disseminate (display) this read-only public PII in order to preserve the rights of these copyright holders.
- Residual privacy risks are mitigated because authenticated (non-public) access to the information will be limited to appropriate NRCS personnel and partners by the use of the USDA-OCIO-eAuthentication application, which provides user authentication for NRCS. Role-Based Access Control (RBAC) provides access enforcement.
- Please see Section 2.4 and Section 8.6 for a further discussion of security controls that are in place to mitigate privacy risks.

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 PII that is maintained by PLANTS includes the names and typical contact information for individuals that hold copyrights for the photographs of plants that are displayed by the PLANTS application.

- To preserve the rights of the copyright holders, PLANTS is required to freely disseminate the public PII information that is maintained within PLANTS.
- The PLANTS application does not make any other use of this public PII.

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

- N/A – PLANTS does not use any type of tools to analyze PII. No PII data is 'produced' and PII data is not manipulated or reformatted.

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

- N/A – PLANTS does not use commercial or publicly available data.

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.

- This application is in compliance with the Federal Information Security Management Act of 2002 (FISMA) as reflected in CSAM, USDA Office of the Chief Information Officer (OCIO) Directives, and National Institute of Standards and Technology (NIST) guidance, including applicable controls provided in these NIST Special Publication 800-53 control families:
  - Access Control (AC)
  - Security Awareness and Training (AT)
  - Identification and Authentication (IA)
  - Media Protection (MP)
  - Physical and Environmental Protection (PE)
  - Personnel Security (PS)
  - Risk Assessment (RA)
  - System and Communication Protection (SC)
  - System and Information Integrity (SI)

  If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

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?

- Application-specific information is retained while the application remains in production. Per NARA General Records Schedule 20, application-specific information has been authorized by the NRCS Records Manager for erasure or deletion when the agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes.

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

- Yes.

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

- Residual privacy risks are mitigated by limited access to the data, non-portability of the data and controlled storage of the data in controlled facilities.
- Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed above.

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 – PLANTS information is not "shared" with any organizations.

4.2 How is the information transmitted or disclosed?

- N/A – PLANTS information is not "transmitted" or "disclosed" to any organizations.

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 PLANTS application does not "share / transmit / disclose" any private (non-public) PII to any other internal USDA organization.
- To preserve the rights of copyright holders, the PLANTS application is required to freely disseminate the public PII information about copyright holders that is maintained in the public web application.
- Privacy risks are mitigated by virtue of NOT sharing information with other internal USDA organizations.
- Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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?

- N/A – PII information is not shared with any organizations.

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.

- N/A – PII information is not shared with any organizations.

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

- N/A – PII information is not shared with or transmitted to any organizations.

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

- PII information is not shared with or transmitted to any organizations.
- To preserve the rights of copyright holders, the PLANTS application is required to freely disseminate the public PII information about copyright holders that is maintained in the public web application.
- Privacy risks are mitigated by virtue of NOT sharing PII with organizations external to USDA.

- Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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?

- N/A – No notice is provided to any individual, because no PII is solicited or collected from any individual by this application.

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

- N/A – No PII is collected from any individual by this 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?

- N/A – No PII is collected from any individual by this application.

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.

- Because no PII is collected from any individual by this application, "Notice" does not need to be provided to any individual.
- There is no risk that any individual would be unaware of "collection," because no PII is collected from any individual by this application.

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?

- N/A – No procedures are required. While no PII is solicited or collected from any individual by this application, individual copyright holders can view their public PII on the public webpages that display their pictures of various plants.

- The PLANTS application does not allow direct input of any PII from any individual (including copyright holders), because the PLANTS web application does not have any user interface (UI) that would allow for any input of any PII.

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

- N/A – No procedures are required. The PLANTS application does not allow direct input of any PII from any individual (including copyright holders), including corrections of inaccurate or erroneous information (e.g., to update an incorrect email address). The PLANTS web application does not have any user interface (UI) that would allow for any input of any PII.

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

- N/A – no notification is provided related to procedures to allow individuals to correct their PII in the PLANTS application, because the individuals associated with any PII in the photographs maintained in PLANTS are not authorized to gain access to PLANTS.
- No PII is collected from any affected individual by this application.

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

- Corrections to photographs and related information (including the PII related to the copyright holder for the photographs) are collected, managed and periodically released by processes that are outside of the accreditation boundary of this application. See Section 1.2.

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 specifically associated with the redress process for this application. There is no risk that an individual would need to correct their PII within the PLANTS application, because no PII is collected from any affected individual by PLANTS. The PLANTS web application does not have any user interface (UI) that would allow for any input of any PII.
- Residual privacy risks associated with the redress process for individual copyright holders are mitigated since individuals can use the relevant procedures discussed above in Section 1.2 to update their original records.

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 the PLANTS application is determined via a valid eAuthentication ID and password (level II) on a valid "need to know" basis, determined by requirements to perform applicable official duties. The application has documented Access Control Procedures, in compliance with FISMA and USDA directives. See Section 2.4.

8.2 Will Department contractors have access to the system?

- No.

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

- NRCS requires that every employee and contractor receives information security awareness training before being granted network and account access, per General Manual, Title 270, Part 409 - Logical Access Control and Account Management.
- Annual Security Awareness and Specialized Training are also required, per FISMA and USDA policy, and this training is tracked by USDA.

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

- Yes. Authority to operate IDEA was granted in 2010.
- An A&A is currently in progress, to be completed by 9/2013.

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

- NRCS complies with the "Federal Information Security Management Act of 2002" (FISMA). Assessment and Accreditation, as well as annual key control self-assessments, and continuous monitoring procedures are implemented for this application per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53. Additionally, NRCS complies with the specific security requirements for "auditing measures and

technical safeguards" provided in OMB M-07-16. Finally, the system provides technical safeguards to prevent misuse of data including:

- Confidentiality: Encryption is implemented to secure data at rest and in transit for this application (e.g., by FIPS 140-2 compliant HTTPS and end-user hard disk encryption).
- Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).
- Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC).
- Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: Logging is implemented for this application (e.g. by logging infrastructure).
- Attack Mitigation: The system implements security mechanisms such as input validation.

Notice: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

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?

- PLANTS does not directly "collect" any PII from any affected individual.
- PLANTS does not "share/transmit" any PII internally (to other USDA agencies) or externally (outside of the USDA). PLANTS does utilize PII within the system which is obtained from other sources (see Section 1.0 above). Data extracts containing PII are not regularly obtained from the system, therefore, privacy risk from this area is limited and addressed through IT Data Extract process controls.
- Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5, and by the security controls discussed in Section 2.4 above. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5 respectively.

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?

- The PLANTS application is an NRCS custom-developed system that has received an Authorization to Operate (ATO), as discussed in Section 8.4.

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

- No. The project utilizes Agency approved technologies, and these technology choices do not raise privacy concerns.

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 - 3rd party websites / applications are not used.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

- N/A - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

- N/A - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

10.10 Does the system use web measurement and customization technology?

- Yes. NRCS will use aggregated web measurement information provided by Google Analytics for the purpose of improving online services through measurement and analysis of public-facing website traffic.
- Google Analytics performs web measurement by gathering feedback using non-identifiable aggregated data such as number of unique visitors to a page and the navigation the visitor took to get to a specific piece of content. The Agency will use this data to make modifications to the website to improve the user experience and monitor the traffic on the website.

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?

- Yes. Users can decline to opt-in (or decide to opt-out) via browser options.
- Google sets a cookie on the user's machine or device. While this cookie is set automatically, the user can "opt-out" if they choose to not have the cookie placed on their machine or device. Making the "opt-out" choice will have no impact on the appearance or functionality of this application's website. The

user may also delete the cookie at any time through the options tab (e.g., in the browser).

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.

- Privacy risks are nominal. Privacy risks associated with Google Analytics web measurement are mitigated, because no Personally Identifiable Information (PII) will become available through the agency's use of Google Analytics.
- NRCS uses non-identifiable aggregated information provided by Google to:
  - Track visits to this application's public-facing facing website(s).
  - Monitor the size of the Department's audience.
  - Better understand the interactions of visitors in order to improve the functionality of this application's public-facing website(s) in order to improve the user experience.
- The PLANTS application does not provide access or link to 3rd party websites or applications. In addition, the PLANTS application does not use customization technology.

Responsible Officials

roel.vining@usda.gov Digitally signed by roel.vining@usda.gov
DN: cn=roel.vining@usda.gov
Date: 2013.08.01 15:58:31 -06'00'

Roel Vining — Date
NRCS
United States Department of Agriculture
This signature certifies that the above PIA responses are provided to the best of my knowledge and understanding.

Approval Signature

8/6/13

Mr. Lian Jin — Date
Acting Chief Information Security Officer
United States Department of Agriculture
This signature certifies that the PTA analysis and PIA determination due diligence has been conducted pursuant to Department guidance and NIST regulations.