



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the [DOI PIA Guide](#) for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: USA National Phenology Network - The Nature's Notebook Plant and Animal Observing Program

Date: March 22, 2017

Bureau/Office: U.S. Geological Survey/Ecosystems Mission Area

Bureau/Office Contact Title: Phenology Program Coordinator

Point of Contact

Email: jweltzin@usgs.gov

First Name: Jake

M.I.: F

Last Name: Weltzin

Phone: (520) 626-3821

Address Line 1: 1311 E 4th Street

Address Line 2: Suite 325

City: Tucson

State/Territory: Arizona

Zip: 85721

Section 1. General System Information

A. Is a full PIA required?

- Yes, information is collected from or maintained on
- Members of the general public
 - Federal personnel and/or Federal contractors



- Volunteers
 All

No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The United States of America National Phenology Network (USA-NPN), established in 2007 by the U.S. Geological Survey (USGS) in collaboration with other governmental and non-governmental organizations, is a national-scale science and monitoring initiative focused on phenology (i.e., the study of seasonal life-cycle events such as leafing, flowering, reproduction and migration) as a tool to understand how plants, animals, and landscapes respond to environmental variation and change. Information collected by the USA-NPN through its national observing system, *Nature's Notebook*, is used by researchers and federal, state, and local agencies and resource managers to: understand and support climate change vulnerability assessments and adaptation; inform management and assessment of habitats and plant and animal species; identify, assess, and forecast change in ecosystems and effects of climate change; identify relationships between environments and wildlife and human health; integrate data and products for science-based stewardship of natural resources; and provide opportunities for public stewardship and engagement.

C. What is the legal authority?

Relevant acts include the Organic Act, 43 U.S.C. 31 et seq., 1879; Fish and Wildlife Coordination Act, 1934; Fish and Wildlife Act, 1956; Migratory Bird Treaty Act, 1918; Migratory Bird Conservation Act, 1900; Federal Land Policy and Management Act, 1976; Fish and Wildlife Improvement Act, 1978; Endangered Species Act, 1973; Marine Mammal Protection Act, 1972; Great Lakes Fishery Act, 1956; Nonindigenous Aquatic Nuisance Prevention and Control Act, 1990; Water Resources Development Act, 1990; and other authorizations conveyed to the U.S. Geological Survey.

D. Why is this PIA being completed or modified?

- New Information System
 New Electronic Collection
 Existing Information System under Periodic Review
 Merging of Systems
 Significantly Modified Information System
 Conversion from Paper to Electronic Records
 Retiring or Decommissioning a System
 Other: *Describe*



E. Is this information system registered in CSAM?

Yes: *Enter the UII Code and the System Security Plan (SSP) Name* 010-000001013 System Security Plan for Science & Support Systems

No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII (Yes/No)	Describe If Yes, provide a description.
None			

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

Yes: *List Privacy Act SORN Identifier(s)* Citizen Science and Crowdsourcing – Interior, GS-29 (Pending)

No

H. Does this information system or electronic collection require an OMB Control Number?

Yes: *Describe* OMB Control Number 1028-0103. Expires 03/31/2019.

No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Truncated SSN |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Legal Status |
| <input type="checkbox"/> Gender | <input type="checkbox"/> Place of Birth |
| <input type="checkbox"/> Birth Date | <input type="checkbox"/> Religious Preference |
| <input type="checkbox"/> Group Affiliation | <input type="checkbox"/> Security Clearance |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Spouse Information |
| <input type="checkbox"/> Biometrics | <input type="checkbox"/> Financial Information |
| <input type="checkbox"/> Other Names Used | <input type="checkbox"/> Medical Information |



-
- | | |
|--|--|
| <input type="checkbox"/> Disability Information | <input type="checkbox"/> Tribal or Other ID Number |
| <input type="checkbox"/> Credit Card Number | <input checked="" type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Law Enforcement | <input type="checkbox"/> Mother's Maiden Name |
| <input type="checkbox"/> Education Information | <input type="checkbox"/> Home Telephone Number |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Child or Dependent Information |
| <input type="checkbox"/> Driver's License | <input type="checkbox"/> Employment Information |
| <input type="checkbox"/> Race/Ethnicity | <input type="checkbox"/> Military Status/Service |
| <input type="checkbox"/> Social Security Number (SSN) | <input type="checkbox"/> Mailing/Home Address |
| <input type="checkbox"/> Personal Cell Telephone Number | |
| <input checked="" type="checkbox"/> Other: <i>Specify the PII collected.</i> Virtual Face or Picture | |

B. What is the source for the PII collected? Indicate all that apply.

- Individual
- Federal agency
- Tribal agency
- Local agency
- DOI records
- Third party source
- State agency
- Other: *Describe*

C. How will the information be collected? Indicate all that apply.

- Paper Format
- Email
- Face-to-Face Contact
- Web site
- Fax
- Telephone Interview
- Information Shared Between Systems
- Other: *Describe* Android and iOS Mobile Apps

D. What is the intended use of the PII collected?

Names, usernames, email addresses, and states are collected to communicate with participants in *Nature's Notebook*. The USA-NPN communicates program updates and contacts participants in the event it is necessary to follow up on observations submitted for further detail. If a participant is affiliated with a group, the group leader uses the name and email to communicate with the participant. Usernames and states are presented on the project leaderboards.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.



- Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*
- Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*
- Other Federal Agencies: *Describe the federal agency and how the data will be used.*
- Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

University of Arizona staff, operating under a Cooperative Agreement with the USGS, which manages *Nature's Notebook*, may access PII to communicate with participants, to provide updates on the program, and to obtain additional information about observation records as necessary.

- Contractor: *Describe the contractor and how the data will be used.*
- Other Third Party Sources: *Describe the third party source and how the data will be used.*

Partners of the USA-NPN, which include nature centers and schools, organize local groups to participate in *Nature's Notebook*. Through communication with USA-NPN staff, a “group” is created in *Nature's Notebook*, and the contact at the partner organization is the administrator of the group. The group administrator then helps observers sign up for *Nature's Notebook* and affiliate themselves with the group. PII for observers affiliated with the group is visible only to the administrator of that group and is used to facilitate communication via email between the group administrator and the group member.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

- Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

A user is able to visit the USA-NPN website without identifying who he or she is or providing any personal information. If the user does decide to register with USA-NPN to facilitate reporting phenological observations or contributing content to the site, the USA-NPN will not sell, trade, or give away the user's personal information, which includes name, username, state, email address, and suggestions or comments made by email. To submit observations to *Nature's Notebook*, participants must provide an email address. Users have the option to opt out of participation in the leaderboards.

- No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*



G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement: *Describe each applicable format.*

Authority: Relevant acts include the Organic Act, 43 U.S.C. 31 et seq., 1879; Fish and Wildlife Coordination Act, 1934; Fish and Wildlife Act, 1956; Migratory Bird Treaty Act, 1918; Migratory Bird Conservation Act, 1900; Federal Land Policy and Management Act, 1976; Fish and Wildlife Improvement Act, 1978; Endangered Species Act, 1973; Marine Mammal Protection Act, 1972; Great Lakes Fishery Act, 1956; Nonindigenous Aquatic Nuisance Prevention and Control Act, 1990; Water Resources Development Act, 1990; and other authorizations conveyed to the U.S. Geological Survey.

Purpose: The USA-NPN collects names, usernames, email addresses, and states to communicate with participants.

Routine Uses: The USA-NPN may communicate program updates and contact participants in the event it is necessary to follow up on observations submitted. If a participant is affiliated with a group, the group leader uses the name and email to communicate with the participant. Usernames and states are presented on the USA-NPN leaderboards. Personal information is not otherwise released to any other party.

Disclosure: Providing this information is voluntary. People may use many of the USA-NPN website tools and services without registration. To submit observations in *Nature's Notebook*, participants must provide a username and email.

Privacy Notice: *Describe each applicable format.*

Other: *Describe each applicable format.*

The USA-NPN website's terms of use contain General Privacy and Observer Privacy policies:

1. General Privacy Policy: <https://www.usanpn.org/terms#GeneralPrivacy>
2. Observer Privacy Policy: <https://www.usanpn.org/terms#ObserverPrivacy>

None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).



Data management staff at the University of Arizona access data using common database queries (text string, numeric ID).

Any website user who downloads phenology data will have access to the unique identification numbers (Observer_ID) of the observers who made and/or submitted the observations downloaded. No other PII is publicly accessible.

Group administrators are presented a list of participants for the group that they manage, but the database is not otherwise searchable.

I. Will reports be produced on individuals?

Yes: *What will be the use of these reports? Who will have access to them?*

No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

All data in the system are self-reported by individual participants. The USA-NPN assumes that contact information provided is accurate. A series of quality assurance and quality control measures are applied to the plant and animal phenology data reported by participants to improve data accuracy and consistency. These measures include allowed value checks on web interfaces and flags applied to conflicting records, and are described in full at: www.usanpn.org/data/quality.

B. How will data be checked for completeness?

Settings on the registration web form prevent incomplete entries of required personal information. Because participation is voluntary and at the discretion of the participant, phenology records may be incomplete (for example, an observer may report on flowering but not fruiting).

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Updated information provided by the participant is immediately updated in the database.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.



Under the USGS General Records Disposition Schedule 101-02 (<https://www2.usgs.gov/usgs-manual/schedule/432-1-s1/ch100a.html#t101>), the retention period for these data is seven years or when superseded, obsolete, or no longer needed, whichever is later.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Electronic data not subject to permanent retention requirements is deleted from the database at the end of the retention period. Procedures for the handling of electronic records are documented in the U.S. Geological Survey Geology Discipline Research Records Schedule: <https://www2.usgs.gov/usgs-manual/schedule/432-1-s5/gd.html#sked>.

Permanent records are cutoff after the completion of the project or when the USA-NPN has no expected research, business, or other purposes for the records, whichever is later, and records are transferred to the National Archives and Records Administration.

F. Briefly describe privacy risks and how information handling practices at each stage of the “information lifecycle” (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a risk to individual privacy because the system contains personal contact information. Participants do also submit information on the location of their observations, but these locations are not necessarily their residences. We have several systems in place to ensure that PII is not made available to unauthorized people. We use a secure HTTPS connection for the web interface and mobile apps to collect the data. When observational data are made available, no personally identifying information about the observer is released. Instead, numeric Observation IDs are provided to data users. Data are stored on servers housed in a secure and conditioned room at the University of Arizona and are located behind a firewall. Software is regularly updated to prevent system vulnerabilities.

Only USA-NPN University of Arizona staff members are able to access the personal information in the database, after logging in with a two-factor authentication system to the University of Arizona VPN. All staff members have undergone Information Security Awareness Training: <https://security.arizona.edu/all-employee-security-awareness>.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

- Yes: *Explanation* The collection of basic PII is necessary for the USA-NPN to meet its mission to collect, store, and share data to support science-based stewardship of natural



resources, and to provide opportunities for public stewardship and engagement. Without this information, it would not be possible to maintain an engaged pool of participants or to follow up with participants for further information about their records.

No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

No

C. Will the new data be placed in the individual's record?

Yes: *Explanation*

No

D. Can the system make determinations about individuals that would not be possible without the new data?

Yes: *Explanation*

No

E. How will the new data be verified for relevance and accuracy?

There is no new data being derived.

F. Are the data or the processes being consolidated?

Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

No, data or processes are not being consolidated.



G. Who will have access to data in the system or electronic collection? Indicate all that apply.

- Users
- Contractors
- Developers
- System Administrator
- Other: *Describe* Group Administrators

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access to all personal information, other than the Observer_ID, is restricted to system administrators on a need-to-know basis. The only exception to this is the personal information about group members that is made available to group administrators.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

- Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*
- No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

- Yes. *Explanation*
- No

K. Will this system provide the capability to identify, locate and monitor individuals?

- Yes. *Explanation* Session information is captured as part of security and troubleshooting. No geographic location information is tracked. The latitude and longitude of observational sites are calculated through Google Maps, but no tracking capability of users is enabled.
- No

L. What kinds of information are collected as a function of the monitoring of individuals?

Logs are used on USA-NPN systems. User actions, such as user ID, log-on date and time, log-off date and time, user actions, and data submission sessions, are recorded in the system audit logs, and the system is monitored for unauthorized access attempts.



M. What controls will be used to prevent unauthorized monitoring?

We ensure that unauthorized monitoring is not occurring through use of HTTPS protocols. Data are stored on servers housed in a secure and conditioned room at the University of Arizona and located behind a firewall. Software is regularly updated to prevent system vulnerabilities. Access to the servers is limited physically and through security configurations for staff with a need-to-know function.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- Security Guards
- Key Guards
- Locked File Cabinets
- Secured Facility
- Closed Circuit Television
- Cipher Locks
- Identification Badges
- Safes
- Combination Locks
- Locked Offices
- Other. *Describe*

(2) Technical Controls. Indicate all that apply.

- Password
- Firewall
- Encryption
- User Identification
- Biometrics
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)
- Public Key Infrastructure (PKI) Certificates
- Personal Identity Verification (PIV) Card
- Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits
- Backups Secured Off-site
- Rules of Behavior



-
- Role-Based Training
 - Regular Monitoring of Users' Security Practices
 - Methods to Ensure Only Authorized Personnel Have Access to PII
 - Encryption of Backups Containing Sensitive Data
 - Mandatory Security, Privacy and Records Management Training
 - Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Ecosystems Associate Director serves as the Information System Owner and the official responsible for oversight and management of the USA-NPN security and privacy controls, including the protection of information processed and stored by the USA-NPN program. The Information System Owner and the USA-NPN Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored by the USA-NPN program. The System Manager is responsible for protecting the privacy rights of the public and employees for the information collected, maintained, and used in the system of records, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the USGS Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The Ecosystems Information System Owner is responsible for oversight and management of the USA-NPN security and privacy controls and for ensuring, to the greatest possible extent, that USA-NPN agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the USGS Computer Security Incident Response Team, preferably by the assigned Security Point of Contact, within one hour of discovery in accordance with Federal policy and established procedures.