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: The National Map Corps

Date: November 21, 2017

Bureau/Office: U.S. Geological Survey/National Map Reengineering Project

Bureau/Office Contact Title: Program Analyst

Point of Contact
Email: amcdonal@usgs.gov
First Name: Anthony
M.I.:
Last Name: McDonald
Phone: (703) 648-5989
Address Line 1: 12201 Sunrise Valley Drive
Address Line 2: Mail Stop 511
City: Reston
State/Territory: Virginia
Zip: 20192

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 U.S. Geological Survey's (USGS) The National Map Corps (TNMCorps) is a component of the National Map Reengineering Project (NMRP) Federal Information Security Modernization Act (FISMA)-reportable information technology system. TNMCorps is operated by the National Geospatial Technical Operations Center (NGTOC) in support of the National Geospatial Program (NGP) and the Core Science Systems Mission Area.

The purpose of TNMCorps is to serve as a crowdsourced mapping project that allows volunteers to assist in collecting and editing man-made structures on an online map. The USGS has developed a customized online editor (https://edits.nationalmap.gov/tnmcorps) to allow volunteers to collect and update different structure feature types, including schools, fire stations, prisons, hospitals, cemeteries, and post offices, in all 50 states, Puerto Rico, and the U.S. Virgin Islands. After going through a tiered quality assurance process, the structures data get incorporated into the *The National Map*.

C. What is the legal authority?

Citizen Science and Crowdsourcing – Interior, GS-30 (Pending): 43 U.S.C. 31 et seq., as amended, Organic Act of March 3, 1879; 44 U.S.C. 3501 et seq., Paperwork Reduction Act of 1980; 44 U.S.C. 2904 and 3102, Federal Records Act of 1950; 5 CFR part 1320, Controlling Paperwork Burdens on the Public; Office of Management and Budget Memorandum M-10-06, *Open Government Directive*; Office of Management and Budget Memorandum M-13-13, *Open Data Policy – Managing Information as an Asset*; Office of Science and Technology Policy Memorandum, *Addressing Societal and Scientific Challenges through Citizen Science and Crowdsourcing*.

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)*

010-000001050 System Security Plan (SSP) for National Map Reengineering Project

☐ 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-30 (Pending)

☐ No

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

☒ Yes: *Describe*

OMB Control Number 1028-0111. Expires 1/31/2018.

☐ No

Section 2. Summary of System Data

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

☐ Name
☐ Citizenship
☐ Gender
☐ Birth Date
☐ Group Affiliation
☐ Marital Status
☐ Biometrics
☐ Other Names Used
☐ Truncated SSN
☐ Legal Status

- ☐ Place of Birth
- ☐ Religious Preference
- ☐ Security Clearance
- ☐ Spouse Information
- ☐ Financial Information
- ☐ Medical Information
- ☐ Disability Information
- ☐ Credit Card Number
- ☐ Law Enforcement
- ☐ Education Information
- ☐ Emergency Contact
- ☐ Driver's License
- ☐ Race/Ethnicity
- ☐ Social Security Number (SSN)
- ☐ Personal Cell Telephone Number
- ☐ Tribal or Other ID Number
- ☒ Personal Email Address
- ☐ Mother's Maiden Name
- ☐ Home Telephone Number
- ☐ Child or Dependent Information
- ☐ Employment Information
- ☐ Military Status/Service
- ☐ Mailing/Home Address
- ☒ Other: *Specify the PII collected.* A username is automatically generated and assigned to a user's profile when signing up for an account. The user can modify his or her username in the profile dashboard. A Twitter handle can also be added by the user as an optional value.

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*

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

Usernames and email addresses are used to contact volunteers about data quality and project updates. Usernames and email lists are maintained on secure servers and within the Department of the Interior (DOI) email client. Twitter handles are optionally provided by volunteers for the

purpose of volunteer recognition via The National Map Twitter account. Volunteers must give permission before USGS will use the Twitter handles.

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.*

Data will be shared with individuals with a need to know within NGP in order to contact volunteers about data quality and project updates.

☐ 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.*

☐ 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.*

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 view the TNMCorps website without identifying who he or she is or providing any personal information. If the user wishes to collect, modify, delete, and verify structures data, then the user must create an Online Editor Account and provide an email address. Upon registering, the user is automatically assigned a username, which can be modified by the user at any time. Users have the option to opt in to authorize the USGS to publish usernames as needed to show contribution achievements via social media and websites.

☐ 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.*

PRIVACY ACT STATEMENT

Authority: This information is solicited under the authority of 43 U.S.C. 31 et seq.; 44 U.S.C. 2904 and 3102; 5 CFR part 1320; Office of Management and Budget Memorandum M-10-06, *Open Government Directive*; Office of Management and Budget Memorandum M-13-13, *Open Data Policy – Managing Information as an Asset*; and Office of Science and Technology Policy Memorandum, *Addressing Societal and Scientific Challenges through Citizen Science and Crowdsourcing*.

Purpose: The purpose of this application is to provide essential support and functionality for the acquisition and management of trusted geospatial data, products, and services in support of *The National Map*.

Routine Uses: Usernames, email addresses, and Twitter handles are shared with the U.S. Geological Survey (USGS) National Geospatial Program to contact volunteers who contribute information through The National Map Corps about data quality and project updates. Usernames may be published (with permission) by the USGS via social media and websites in order to recognize contributor achievements.

Disclosure: Furnishing this information is voluntary. If the individual does not furnish the information requested, there will be no adverse consequences. However, failure to provide an email address will result in ineligibility to participate in the volunteer program.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the publication of this Privacy Impact Assessment. The required USGS Privacy Notice is linked to web pages. A bimonthly newsletter is also distributed to inform volunteers about the TNMCorps project, changes to the mapping application, data collection strategies, mapping challenges, recognize high achievers, publish articles submitted by volunteers (with permission to publish), and generally engage and interest volunteers in the TNMCorps project. Volunteers may request to be removed from the newsletter distribution emails.

☐ Other: *Describe each applicable format.*

☐ None

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

Only the username and email address are used to retrieve data.

I. Will reports be produced on individuals?

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

Information retrieved via the username or email address is used to produce reports about the number of edits and contributions made by a particular volunteer.

☐ No

Section 3. Attributes of System Data

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

Volunteers are responsible for verifying the accuracy of their data.

B. How will data be checked for completeness?

Volunteers are responsible for verifying the completeness of their data.

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

Volunteers are responsible for ensuring their data is current.

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

Records in this system are maintained under the USGS General Records Disposition Schedule (GRDS) 202-06b - User Identification, Profiles, Authorizations, and Password Files, Excluding Records Relating to Electronic Signatures. GRDS 202-06b is a USGS-wide records schedule that covers routine systems not requiring special accountability, e.g, those containing information that may be needed for audit or investigative purposes and those that contain classified records. The disposition for these records is temporary, and the records are destroyed when the bureau determines they are no longer needed for administrative, legal, audit, or other operational purposes.

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

User information is retained for only as long as the user is actively participating in the project. For inactive accounts, electronic records shall be deleted. Users are reviewed on a yearly basis to determine if an editor is still participating in the TNMCorps project and to determine if a user's information should be removed from the record. User information will be removed at any time at the request of the user. The username associated with a specific data edit is retained for the duration of the TNMCorps project for recognition purposes.

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 in the form of usernames, email addresses, and Twitter handles. Privacy risks include inadvertent disclosure or a malicious attack on systems. Systems are secured through the DOI Assessment and Authorization program. Web applications and hardware are secured through the use of USGS Security Technical Implementation Guides and are assessed through a program of continuous monitoring that includes monthly vulnerability scans. Developers, system administrators, and database administrators complete annual Information Management and Technology (IMT) Awareness Training and agree to the DOI Rules of Behavior as a condition of training completion. Personal data that has become obsolete will be deleted by the responsible individual. Data that has been backed up will be either overwritten by the tape rotation cycle or the backup media will be properly destroyed. System hard drives are overwritten prior to reuse and scrubbed prior to decommissioning. Procedures are documented in the individual System of Records Notice. TNMCorps information is retained only as long as the user is actively participating in the project.

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* Usernames and email addresses are used to contact volunteers about data quality and project updates. Usernames and email lists are maintained on secure servers and within the DOI email client. Twitter handles can be voluntarily submitted by the user for the purpose of volunteer recognition via The National Map Twitter account. Volunteers must give permission before USGS will use the Twitter handles.

☐ 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?

Not applicable; this system does not derive new data or create previously unavailable data about an individual through data aggregation.

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*

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

Users have access to their own data. Access to all other personal information is restricted to system administrators on a need-to-know basis.

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?* Yes

☐ 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* The TNM Corps application stores information associated with a data edit submitted by a volunteer, which includes username, user email, time and date associated with a data edit, and the last time a user logged into the application.

☐ No

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

The TNM Corps application stores information associated with a data edit submitted by a volunteer, which includes username, user email, time and date associated with a data edit, and the last time a user logged into the application. The system is monitored for unauthorized access attempts.

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

Access control lists are in place to guard against unauthorized access. The TNMCorps system is protected from unauthorized access by firewalls, intrusion detection systems, antivirus programs, and the inherent security of the Active Directory domain environment. To mitigate the insider threat, collected data is protected by a combination of user ID, user password, and limited restricted access. Employees are required to complete the yearly IMT Awareness Training, which includes affirming the USGS Rules of Behavior. Audit logs for the data are reviewed regularly for anomalies. USGS computers are secured and scanned monthly in accordance with the USGS Continuous Monitoring Program Plan.

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 NGTOC Director serves as the Information System Owner and the official responsible for oversight and management of the TNMCorps security and privacy controls, including the protection of information processed and stored by the TNMCorps program. The Information System Owner and the Information System Security Officer 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 TNMCorps 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 Information System Owner is responsible for oversight and management of the TNMCorps security and privacy controls and for ensuring, to the greatest possible extent, that TNMCorps 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 immediately to the USGS Computer Security Incident Response Team, whether suspected or confirmed, in accordance with Federal policy and established procedures.

Section 5. Review and Approval

PIAs for Bureau or Office level systems must be signed by the designated Information System Owner, Information System Security Officer, and Bureau Privacy Officer, and approved by the Bureau Assistant Director for Information Resources as the Reviewing Official. Department-wide PIAs must be signed by the designated Information System Owner, Information System Security Officer, and Departmental Privacy Officer, and approved by the DOI Chief Information Officer/Senior Agency Official for Privacy as the Reviewing Official.

Information System Owner

Name: Kari J. Craun
Title: Director, National Geosptial Technical Operations Center
Bureau/Office: U.S. Geological Survey/Core Science Systems
Phone: (573) 308-3802 Email: kcraun@usgs.gov

Signature: KARI CRAUN Digitally signed by KARI CRAUN DN: c=US, o=U.S. Government, ou=Department of the Interior, ou=Geological Survey, cn=KARI CRAUN, 0.9.2342.19200300.100.1.1=14001000295101 Date: 2017.11.21 12:49:31 -06'00' Date: _____

Information System Security Officer

Name: Anthony McDonald
Title: Program Analyst
Bureau/Office: U.S. Geological Survey/Core Science Systems
Phone: (703) 648-5958 Email: amcdonal@usgs.gov

Signature: ANTHONY MCDONALD Digitally signed by ANTHONY MCDONALD Date: 2017.11.21 13:20:09 -05'00' Date: _____

Privacy Officer

Name: James Piyavansuthi
Title: Associate Privacy Officer (Acting)
Bureau/Office: U.S. Geological Survey/Office of Enterprise Information
Phone: (703) 648-7017 Email: jpiyavansuthi@usgs.gov

Signature: _____ Date: _____

Reviewing Official

Name: Timothy S. Quinn

Title: Associate Chief Information Officer
Bureau/Office: U.S. Geological Survey/Office of Enterprise Information
Phone: (703) 648-6839 Email: tsquinn@usgs.gov

Signature: _____ Date: _____