U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires Privacy Impact Assessments (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: National Map Reengineering Project
Bureau/Office: U.S. Geological Survey/Core Science Systems
Date: September 13, 2019
Point of Contact:
Name: Cozenja M. Berry
Title: Associate Privacy Officer
Email: privacy@usgs.gov
Phone: 703-648-7062
Address: 12201 Sunrise Valley Drive Suite MS-521, Reston, VA 20191

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 National Map Reengineering Project (NMRP) boundary is a USGS a General Support System (GSS) that hosts Information (IT) technology infrastructure and platforms required to support The National Map's mission. It is comprised of components at two National Geospatial Technical Operations Center (NGTOC) locations. Pursuant to The National Map's mission, the suite of products and services in this boundary provide access to base geospatial information that describes the landscape of the United States and its territories. Collectively, NMRP systems are used to acquire, manage, archive, and deliver data products associated with The National Map. Important functions that support these activities are computer systems development, systems testing, and data visualization. The primary data types include: elevation data; vector data for hydrography, transportation, boundary, and structure features; geographic names; and land cover information. Within NMRP, personally identifiable information (PII) is maintained within The National Map Corps (TNMCorps, https://edits.nationalmap.gov/tnmcorps/). TNMCorps is NMRP's online crowdsourcing mapping project that allows volunteers to report and update man-made structures data, including schools, fire stations, hospitals, cemeteries, and post offices. Volunteers are assigned a username upon signing up and have the option of providing a Twitter handle which is used for volunteer recognition on social media. Email addresses are used to contact volunteers about data quality and to receive project updates.

C. What is the legal authority?

15 U.S.C. 3724: Crowdsourcing and citizen science; 43 U.S.C. 31: Director of United States Geological Survey; 43 U.S.C. 31a: Findings and purpose; 43 U.S.C. 31c: Geologic mapping program; 43 U.S.C. 31e: Geologic mapping program 5-year plan; 43 U.S.C. 31f: National geologic map database; OMB Circular No. A-16 Revised, Coordination of Geographic Information and Related Spatial Data Activities; OMB Circular A-130 – Management of Federal Information Resources; OMB M–10–22, Guidance for Online Use of Web Measurement and Customization Technologies, June 25, 2010.

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)*

Records are maintained under the following system of records notices: DOI-08, DOI Social Networks (July 22, 2011, 76 FR 44033); DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) (March 12, 2007, 72 FR 11040); and GS-18, Computer Registration System (May 19, 2009, 74 FR 23430). The GS-18, Computer Registration, SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108. These SORNs may be viewed on the DOI SORN website at: https://www.doi.gov/privacy/sorn.

☐No

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

☒Yes: *Describe*

TNMCorps' OMB Control Number is 1028-0111 with an expiration date of 04/30/2021.

☐No

Section 2. Summary of System Data

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

☒Name
☒Personal Email Address
☒Other: *Specify the PII collected.* A computer ID (CUID) is automatically assigned to a user's profile when registering for an account in TNMCorps. The CUID is then changed to a standard username by the user. A Twitter handle can also be added by the user but is not required.

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?

TNMCorps uses usernames and email addresses 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 to be recognized via *The National Map* Twitter account. Volunteers must provide permission before the USGS publishes usernames or Twitter handles. 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 opt out of the newsletter distribution emails.

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.*

For TNMCorps, data may be shared within the National Geospatial Program with individuals on a need-to-know basis 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.*

Information may be shared with other Federal agencies as authorized pursuant to the routine uses contained in the applicable System of Records Notices (SORNs).

☒Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Information may be shared with Tribal, State, or Local agencies as authorized pursuant to the routine uses contained in the applicable SORNs.

☒Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with contractors who perform services or otherwise support USGS activities related to NMRP, and as authorized pursuant to the routine uses contained in the applicable SORNs.

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

Twitter handle may be shared with the public for individual recognition and authorized pursuant to the routine uses contained in the applicable SORNs.

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.*

For TNMCorps, individuals have the right to decline to provide information at the time of the information request. Individuals volunteering with TNMCorps can decline by not proceeding with entering the information into the web interface. Federal, State, and Local partners have the option not to enter into agreements with the USGS.

☐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.*

Individuals are provided notice through a Privacy Act Statement published on TNMCorps' web page (https://my.usgs.gov/confluence/display/nationalmapcorps/Privacy+Statement).

☒Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the publication of this Privacy Impact Assessment and the published system of records notices. The required USGS Privacy Notice is linked to web pages.

☐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.).

TNMCorps uses only the username and email address 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?*

TNMCorps produces reports about the number of edits or 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 and Federal, State, and Local partners are responsible for updating or changing their information in TNMCorps

B. How will data be checked for completeness?

For TNMCorps, volunteers and Federal, State, and Local partners 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).

For TNMCorps, volunteers and Federal, State, and Local partners 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.

For TNMCorps, user registration records are maintained under the USGS General Records Disposition Schedule, Item 202-06b - User Identification, Profiles, Authorizations, and Password Files, Excluding Records Relating to Electronic Signatures. The disposition of 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.

Cartographic data within NMRP is maintained under 1703-01c. Master File for Cartographic Data. PERMANENT. One time transfer. Transfer copy to NARA upon approval of this schedule. Transfer to NARA in accordance with 36 CFR 1228.270, or whatever NARA transfer guidance in effect at the time of the transfer.

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

For TNMCorps, user registration is retained only for as long as the user is actively participating in the project. For inactive accounts, electronic records shall be deleted. Backup tapes are degaussed and reused. These procedures comply with the National Institute of Standards and Technology Special Publication 800-53 and are documented in section MP-06 of the USGS Standard Operating Procedures for Media Protection (MP).

TNMCorps reviews users on a yearly basis to determine if an editor is still participating in the 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 minimal risk to individual privacy as TNMCorps only collects 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. 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 associated SORNs.

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*

TNMCorps uses usernames and email addresses 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 voluntarily be submitted by the user for volunteer recognition purposes via *The National Map* Twitter account. Volunteers must provide permission before the USGS publishes usernames or 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 and other individual's usernames. 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?*

The USGS IT Statement of Work is used to ensure the necessary Privacy Act clauses are included in the procurement of contractor services.

☐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 TNMCorps 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?

Audit trails of user activity are kept. Invalid logon attempts are recorded. An edit history for each feature is created and associated with the username. System auditing follows the USGS guidance for the National Institute of Standards and Technology Special Publication 800-53 Auditing controls and includes at a minimum what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identify of any user/subject associated with the event. The TNMCorps 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. NMRP systems are protected from unauthorized monitoring 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 Director of the National Geospatial Technical Operations Center (NGTOC) serves as the NMRP Information System Owner (ISO) and the official responsible for oversight and management of the NMRP security controls and the protection of agency information processed and stored by NMRP. The ISO and the NMRP Information System Security Officer (ISSO) 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 within the NMRP boundary. 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. The System Manager is also responsible 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 Associate 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 NMRP ISO is responsible for oversight and management of the NMRP program security and privacy controls and for ensuring, to the greatest possible extent, that NMRP program data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The ISO is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of customer agency and agency PII is reported to the customer agency and the USGS Computer Security Incident Response Team immediately upon discovery in accordance with Federal policy and established procedures.