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: Bureau of Reclamation Geographic Information System (BORGIS)
Bureau/Office: Bureau of Reclamation/Denver Office
Date: 4/19/2018
Point of Contact:
Name: Regina Magno
Title: Associate Privacy Officer
Email: privacy@usbr.gov
Phone: 303-445-3326
Address: PO Box 25007, Denver, CO 80225

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 Bureau of Reclamation Geographic Information System (BORGIS) is a geospatial data management system used to create, store, maintain, analyze, retrieve, and deliver geospatial feature data along with associated data attributes required by the Bureau of Reclamation programs and offices in conducting and supporting mission accomplishment. The system supports field to enterprise workflows presenting consistent geospatial data and associated data to applications on mobile, web, and desktop platforms. BORGIS reduces data duplication, improves data quality and streamlines access to Reclamation's geospatial data assets through a suite of off-the-shelf and custom applications designed to meet program day-to-day operations and mandated reporting requirements.

BORGIS is a distributed client-server system that supports the acquisition, processing, storage, retrieval, and delivery of Reclamation geospatial data and imagery assets. The system provides a wide variety of services including, but not limited to, geospatial data storage and retrieval, web mapping services, geoprocessing, spatial analysis, data visualization, and cartographic map products.

The system delivers geospatial data and services that directly support Reclamation business functions and operations associated with real property asset management, land and resource management planning, water resource management and operations, Endangered Species Act activities, National Environmental Policy Act (NEPA) documentation, environmental site analysis, cultural resource management, geological investigations, hydrologic modeling, facility operations and maintenance activities, cartographic production and illustration, and other related uses of geospatial data analysis and mapping.

C. What is the legal authority?

Executive Order 12906, *Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure*, amended by Executive Order 13286, *Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*; Executive Order 12951, *Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems*; OMB Circular A-16, *Coordination of Geographic Information and Related Spatial Data Activities*; OMB Circular A-130, *Managing Information as a Strategic Resource*

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?

The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

☒ Yes: 010-000000274; Bureau of Reclamation Geographic Information System (BORGIS) System Security Plan

☐ 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	**None**	No	**N/A**

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)*
☒ No

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

☐ Yes: *Describe*
☒ No

Note: This system is not a Privacy Act system and does not maintain records on individuals, however, employee names, usernames and contact information are covered under the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS)" system of records notice.

Section 2. Summary of System Data

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

☒ Name
☒ Mailing/Home Address
☒ Other: This system collects employee name, username, supervisor's name, work phone and work email address, as well as access level for the authorized system users. Other types of PII, such as individual name and address, included in public records obtained from publicly available sources may be used in mapping for authorized purposes to conduct land and water resource management activities required to support Reclamation's mission. The system only allows the authorized user to see PII, and the system only stores PII and does not modify or maintain the PII. A user can only download or print cartographic products or illustrations generated by the system that may display the individual name and/or address as found in public records data.

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: Individual names and addresses are obtained from public land records maintained by state and county government offices.

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:

The system allows users to access to publicly available web services that may contain individual names and addresses stored in public land records maintained by state and county government offices.

Authorized user's name and username is extracted from system integration with the DOI Enterprise Active Directory (EAD) system, which authenticates users on the network. When a user logs in and navigates through the system their "user name" and name will be captured in system audit logs. System logs provide a chronological record of information system activities, including records of system accesses and operations performed in a given period. In order to set up permissions within the application names of individual users are associated with folders/groups that determine permission/access.

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

Individual name and address obtained from public records is used in geospatial analysis or mapping to support Reclamation mission activities related to water distribution and power generation. PII is used by Reclamation personnel in support administration and operations activities, including: real property asset management, land and resource management planning, water resource management and operations, environmental site analysis, cultural resource management, geological investigations, hydrologic modeling, and facility operations and maintenance activities. PII may be used to generate products including cartographic production, illustration, transaction document exhibits, and notifications.

Employee user data is used to identify system users and their group memberships to implement appropriate access controls, to facilitate storage and retrieval of user-managed content and data, and to log data creation and modification by users (username and date).

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

☒ Within the Bureau/Office:

BOR System Administrators (authorized employees only) manage user access, review and analyze user account information (name, username, login dates, access attempts, etc.) against operating system and security events when providing help desk support, and report inappropriate or unusual activity to designated DOI officials.

☐ 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:

User information is voluntarily provided by employees when requesting access to the DOI network and information systems. This normally occurs during the onboarding process and is required to create user accounts in the EAD system and enforce access controls across the DOI network. If users decline to provide the requested information they will not be given access to the DOI network or information system.

☒ No: Individual names and addresses are obtained from public records, not directly from individuals.

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 Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA. Employees may also view the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice for more information on how DOI network user accounts are managed.

☒ Other:

When a user logs on to their computer the DOI Warning Banner appears which states the user understands all activity is tracked and not private.

> **WARNING TO USERS OF THIS SYSTEM**
> This computer system, including all related equipment, networks, and network devices (including Internet access) is provided by the Department of Interior

(DOI) in accordance with the agency policy for official use and limited personal use.

All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system.

By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action.
Unauthorized or illegal use may subject you to prosecution.

☐ None

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

PII, such as individual name and address, included in public records are obtained from publicly available sources, and are based on map location and are not stored on the system. Map location can be used to retrieve an associated individual name or address. PII is displayed by land parcel or feature such as canal. Land owner records and transaction records are generally retrieved by location, but may be retrieved by name.

System user data is retrieved by employee username in EAD.

I. Will reports be produced on individuals?

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

Reports are not produced on individuals but on the actions of system users. If actions show unusual or malicious, etc. behavior, the logs can correlate the actions taken in the system with a username. Reports can be generated to include any of the following events: successful and unsuccessful account logon events, account management events, object access, and privilege functions. Only systems administrators and the information system owner will have access to the activity reports.

☐ No

Section 3. Attributes of System Data

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

Data obtained from public land records are not verified for accuracy and is presumed to be accurate as it is maintained by local or county government agencies.

B. How will data be checked for completeness?

Data obtained from public land records is presumed to be complete as it is maintained by local or county government agencies. There is no way to verify the completeness of public records obtained from public sources. Employee user account information is authenticated against Enterprise Active Directory records, and the documented list of authorized individuals is updated annually.

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

Data obtained from public sources is acquired as needed based on Reclamation mission requirements, and is presumed to be current at the time it is obtained as it is maintained by local or county government agencies. BORGIS does not modify or maintain PII data in EAD. PII data in EAD is maintained by Reclamation Active Directory domain administrators.

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 covered under Reclamation records retention schedule PRJ-26.00 GIS (Geographic Information System) by the National Archives and Records Administration (NARA) approval authority N1-115-94-8, which is being incorporated into the Departmental Records Schedule (DRS) 2.4.2.12 “Mission - Provide a Scientific Foundation for Decision Making - Geospatial Services”, which is currently pending approval by NARA. Records retention is permanent under the current Reclamation retention schedule. When NARA approves DRS-2, BORGIS records will be permanent. Records will be cutoff at the end of the fiscal year. Records will be transferred to the Federal Records Center at 10 years or earlier if volume warrants. Transfer legal ownership to NARA 15 years after cutoff.

Records on user activity are retained in accordance with DRS – 1, Administrative schedule 1.4 A.1 – [0013] Short Term IT Records – System Maintenance and Use

Records (DAA-0048-2013-0001-0013). These records have a temporary disposition. Records are cut-off when obsolete and destroyed no later than 3 years after cut-off.

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

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1. Data Archive and Disposal procedures are documented in *BORGIS SOP Data Management*, which is available as an artifact in CSAM.

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.

Land owner name and address from publicly available sources poses no greater risk to individual privacy than the publicly available sources from which PII is obtained. However, there is a limited risk to the privacy of individuals for the use in BORGIS associated with land owner and transaction records. There is a risk that PII could be inappropriately accessed or used for unauthorized purposes. PII is utilized by Reclamation personnel for authorized uses in support of administration and operations activities, including: real property asset management, land and resource management planning, water resource management and operations, environmental site analysis, cultural resource management, geological investigations, hydrologic modeling, and facility operations and maintenance activities.

System users may display individual name and/or address as found in public records data in cartographic products or illustrations generated by the system. PII may be used to generate products including cartographic production, illustration, transaction document exhibits, and notifications. PII is not shared outside Reclamation, unless required by law. Requests for PII obtained from public sources are directed to the original public source.

There is a risk that PII will be maintained for longer than necessary to meet operational or mission requirements. BORGIS records are permanent records due to their historical significance and importance as scientific foundation for decision making. This system provides users with access to publicly available web services of high resolution aerial or satellite imagery base maps that may pose some privacy risk due to level of detail sufficient that may allow users to identify or locate individual properties or other on the ground features. Imagery is routinely used as a base map to provide context and to locate Reclamation real property assets to determine how they relate to proximate public and private property. However, these products are used and accessed internally by authorized users and are not released to the public. PII is not shared outside Reclamation, unless required by law.

BORGIS temporarily stores username for Federal employees, and contractors working on behalf of Reclamation, who access, use and contribute to data stored in the system. BORGIS has implemented privacy and security controls to minimize risk individual privacy risks. BORGIS uses the NIST SP 800-53 rev. 4 security controls, and follows NIST guidelines in implementing and managing its security policies and privacy controls. The transmission of the data is protected through the use of secure based protocols, and the data stored is protected though locally encrypted device management. BORGIS has a FISMA rating of Moderate based upon the type and sensitivity of data, and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. A FISMA Moderate Authority to Operate is expected to be completed by December 2018.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. Continuous monitoring scripts automatically capture user audit logs which contain user login information, such as successful logins, failed logins, and account lockouts for the past 30 days. Audit trails of activity are maintained to reconstruct security relevant events. The audit trail will include the identity of each user accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to the project manager who will report it to local and/or regional IT Security.

BORGIS follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Reclamation employees and contractors are required to complete security and privacy awareness training and sign the DOI Rules of Behavior.

All user information is captured in the audit logs and the system is protected by giving access only to valid, authorized personnel. This information is not shared outside of Reclamation as the system is for internal use only. Backups of the data can only be accessed by valid, authorized users within Reclamation. When the system reaches end of life the equipment and/or media that contains user information and audit logs will be retained in accordance with the records retention schedule for Information Technology systems.

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: BORGIS provides the capability for system users to create maps, illustrations, exhibits that may contain PII required in the of performance of administration and operations activities.

Username is required to facilitate storage and retrieval of user-created content and data, and to check group membership to implement access controls.

☐ 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. BORGIS does not derive new data.

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?

Access to data is restricted through permissions and access controls. System administrators have access based on a need to know and least privilege principle.

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. Privacy Act contract clauses are included in the contract. Contractors involved with the system work and possess the same security access as employees (i.e., ID badge, PIV, DOI Active Directory account, background check).

☐ 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 system provides the capability to find a map location by land owner address obtained from public records. The system does not provide the capability to monitor individuals based PII contained in publicly available records.

This system provides the capability for identifying individuals by employee username in the system, for the purpose of authenticating and monitoring the user's activities on the system through audit logs.

☐ No

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

Employee user activity information is collected by BORGIS system logs in compliance with NIST 800-53 security controls; and includes: username, date and time of login, computer hostname, failed login attempts, and account lockouts.

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

Reclamation complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Quarterly scans are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration. The use of DOI and Reclamation IT systems is conducted in accordance with the appropriate DOI and Reclamation use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events, and will include the identity of users accessing the system, time and date of access (including activities performed using a system administrator's identification), and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Only authorized users with system administrator privileges have access to monitor user's activities in the system. The BORGIS follows the NIST 800-53 controls and DOI security and privacy control standards for user access based on least privilege, ensuring that only authorized individuals are authorized to have access to system data.

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

(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 Lower Colorado Region, Regional Director serves as the BORGIS Information System Owner and the official responsible for oversight and management of the security and privacy controls for the system. The Information System Owner and the Information System Security Officer, in collaboration with the BOR Associate Privacy Officer, are responsible for ensuring adequate safeguards are implemented in compliance with Federal laws and policies for the data managed and stored in BORGIS.

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 BORGIS Information System Owner is responsible for oversight and management of the BORGIS security and privacy controls, and for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner is also responsible for reporting any loss, compromise, or unauthorized access to the system or data to the DOI Computer Incident Response Center within one hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any potential compromise in consultation with the the BOR Associate Privacy Officer.