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: National Irrigation Information Management System (NIIMS 5.0)
Bureau/Office: Bureau of Indian Affairs (BIA)/Trust Services, Branch of Irrigation and Power
Date: January 29, 2025
Point of Contact
Name: Richard Gibbs
Title: Indian Affairs (IA) Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 445-0854
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

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 BIA completed a Privacy Threshold Analysis (PTA) on September 12, 2023, which indicated an update to the previous Privacy Impact Assessment (PIA) was needed. This PIA is being completed to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559), the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101), and Privacy Act of 1974, as amended (5 U.S.C. §552a).

The BIA Office of Trust Services, Division of Water and Power's mission is to promote self-determination, economic opportunities, and public safety through the sound management of irrigation, dam, and power facilities owned or operated by BIA.

The NIIMS is a major application developed to ensure compliance with 25 CFR 171, Irrigation Operations and Maintenance. NIIMS is a collection, debt management, and billing system used for Indian irrigation projects operated by the BIA. The system facilitates the revenue and collections business cycle, including billing for the construction, operation and maintenance costs of the project which are reimbursable to the Federal government.

The NIIMS uses Active Directory (AD) authentication. AD authentication for User access is covered under the Department of the Interior (DOI) Enterprise Hosted Infrastructure (EHI) PIA. For additional information on user authentication please see the EHI PIA on the DOI Privacy website: www.doi.gov/privacy/pia.

This updated PIA is being conducted to evaluate risks related to the current NIIMS system (periodic update) and its NIIMS 5.0 upgrade and migration to a new vendor hosted by a cloud service provider. To meet the requirements of Executive Order (EO) 14028 and OMB M-22-09 for Zero Trust and application layer phishing-resistant Multifactor Authentication (MFA), the legacy NIIMS v1.9.1 system will be modernized to NIIMS 5.0, a Microsoft Dynamics 365 Software-as-a-service (SaaS) application and/or service. Microsoft SharePoint and Power Automate for Government will also be used to store and share data, and data automation tool for integration purposes. The applications will be hosted in the Microsoft Government Community Cloud. A decommissioning PIA will be completed on the current system in use once the migration has been completed.

C. What is the legal authority?

25 U.S.C. Chapter 11, Irrigation of Allotted Lands; 31 U.S.C. 3711, Collection and Compromise; and 25 CFR Part 171, Irrigation Operations and Maintenance; Water Infrastructure Improvements for the Nation Act of 2016 (Pub. L. 114-322 (WIIN Act)), Sections 3101 and 3222.

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 Bison Governance, Risk, and Compliance (Bison GRC) platform?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-000000070, NIIMS 5.0, System Security and Privacy Plan (SSPP)

☐ 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.*
Power Apps PTA completed September 12, 2023	Development of NIIMS 5.0 modernization project.	Yes	All PII data elements indicted in Section 2.A. below.
Microsoft SharePoint Online	Document capture and storage.	Yes	All PII data elements indicted in Section 2.A. below.
Microsoft Power Automate for Government	Data automation tool used for integration purposes.	Yes	All PII data elements indicted in Section 2.A. below.

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)*

INTERIOR/BIA-34, National Irrigation Information Management System (NIIMS), 78 FR 7804 (February 4, 2013), modification published at 86 FR 50156 (September 7, 2021), covers records of current and former landowners and lessees, Federal employees, state and local government employees, Tribal government officials, and other individuals responsible for reimbursing the government for the construction of Indian Irrigation Projects or to whom the operation and maintenance costs of the projects have been or will be assessed, and other individuals with whom business is conducted. This SORN may be viewed at https://www.doi.gov/privacy/sorn.

INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021), covers how DOI collects information from personnel to provide authorized individuals with access to DOI information technology IT resources.

DOI SORNs are available for review on the DOI-Wide SORNs Web page at https://www.doi.gov/privacy/sorn.

☐ No

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

☒ Yes: *Describe*

OMB Control Number 1076-0141, Water Request, Expires March 31, 2026, which includes the following forms.

- Request for Irrigation Services (BIA-DWP-Irr-101)
- Request for Customer Information (BIA-DWP-Irr-102)
- Annual Assessment Waiver Application (BIA-DWP-Irr-103)

- Incentive Agreement (BIA-DWP-Irr-104)
- Land Classification/Designation Application (BIA-DWP-Irr-105)
- Agreement for Carriage of Water (BIA-DWP-lrr-106)

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Birth Date
☒ Group Affiliation
☒ Other Names Used
☒ Spouse Information
☒ Financial Information
☒ Credit Card Number
☒ Race/Ethnicity (Whether the individual is a member of a Tribe.)
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

This system contains records such as, deeds, maps, land surveys, leases, land designation, land re-designation records reflecting current and former owners of land and lessees on which Indian Irrigation projects are constructed, including name, SSN, account/ID, whether the owner is a Federal entity (exempt from certain collection actions), Indian (pertinent to revenue classification), or whether the land is fee or trust, tax identification number, Indian identification number, owner or customer identification number, phone number, name, address, permits and leases.

Billing information, including name of debtor, address, tax identification number, SSN, business phone, fax number, date of death, bankruptcy filing information, ownership interests, rate billed, amount charged, interest and penalty, collection actions, name of the person who remits payment, check number, bank routing and account number, and amount paid.

Information about land on which irrigation projects are constructed, including land construction data, county assigned district identifier, acreage, description of location, name of owner or lessee, water delivery location, time and date of requested water delivery, duration of water delivery, rate of water flow, crop statistics, and the value of the construction debt allocated to the land.

Pursuant to the Debt Collection Improvement Act of 1996 (Public Law 104-134), individuals and organizations doing business with the government are required to furnish their SSN or taxpayer identification number (TIN).

NIIMS may also contain non-sensitive, business-related contact information of company representatives that are not subject to the Privacy Act, as well as data on a small proportion of sole proprietors, which are covered by the Privacy Act. Records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information.

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: Information in the system is obtained directly from current and former landowners and lessees, state and local government employees, individuals responsible for reimbursing the government for constructing Indian irrigation projects, or to whom the projects' operation and maintenance costs have been or will be assessed, and other individuals with whom business is conducted. Information may be manually extracted from other in-house BIA records and may include realty and probate records, records obtained from county assessors and title companies, tribal documents, and information collected via the United States (U.S.) Department of Treasury.

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 *Describe*

Trust Asset and Accounting Management System (TAAMS). Name, addresses, TIN, Tribal Enrollment ID, land ownership and lease information, date of death, and date of birth are manually entered into NIIMS by an authorized user.

Financial and Business Management System (FBMS). The FBMS is an enterprise-wide financial management system that consolidates the majority of the Department of the Interior's (DOI) business and financial management functions. Daily financial transactions are generated by NIIMS, summarized, and uploaded to FBMS. The transaction is completed via an automated nightly interface file Secure File Transfer Protocol (SFTP) upload. Transactions are summarized by project, transaction code and revenue source code and do not contain PII.

Pay.gov. Pay.gov is a free and secure service that allows you to pay many, but not all, United States Government agencies. Pay.gov uses the latest industry-standard methods and encryption to safely collect, store, transmit, and protect all information submitted. Bank and card account numbers are encrypted on Pay.gov and are masked with asterisks (*) when displayed. Checks,

money orders, and credit card payments from Pay.gov are processed by certified Collection Officers, entered in NIIMS via a secure SFTP, and bill balances due are updated.

Cross System Next Generation (CSNG). The purpose of the CSNG system, which is managed by the Department of the Treasury's Bureau of Fiscal Service, is to maintain records about individuals who owe delinquent non-tax debt(s) to the U.S. Government referred for collection by departmental and program agencies (Creditor Agencies). Outstanding past due debt is referred monthly to the Department of Treasury for cross-servicing, or further debt collection processing via a SFTP batch transmission interface. This is in support of debt management practices required by Debt Collection and Improvement Act of 1996 and DOI.

OTCnet. The Over-the-Counter Channel Application (OTCnet), which is managed by the Department of the Treasury's Bureau of Fiscal Service, is a web-based application that offers federal agencies flexible solutions to streamline management and reporting of payment transactions and deposits. OTCnet provides an all-in-one platform to automate deposit and payment processes, simplifying the classification of Treasury collections.

U.S. Bank (Lock Box). The General Lockbox Network (GLN or Lockbox) is the mail in channel for collecting and processing BIA NIIMS irrigation customer payments. US Bank is the vendor/provider that scans and captures paper payment, check deposit, and remittances. Data and images are electronically transmitted to BIA. Using a script and the built-in import functionality, NIIMS 5.0 will receive an eXtensible Markup Language (XML) file based on the import requirements of US Bank. The file will be received nightly and saved to a pre-designated file share location. The Lockbox promotes reduction of in-house paper payment handling processes.

☐ Other: *Describe*

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

The collected PII is used for billing owners or lessees of irrigable land for costs that are reimbursable to the U.S. Government, and for collection actions required by Federal regulations in the event of non-payment, for servicing the account, and for water delivery.

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.*

The data is shared with DOI employees acting in their official capacity for entry and reference in various processes including payment plan eligibility, disputes, refunds, and payment processing. Information may be shared with the BIA Realty office for notifications of a failure to pay an operation and maintenance bill related to a lease of land in trust or restricted status as this is a violation of such a lease. PII data is shared with irrigation project offices, which report to the Field Operations Deputy Director, for conducting irrigation business. System administrators have access to system data and system audit logs to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions. PII data is shared with geospatial staff, which report to the Division of Water and Power, for creating multi-layered maps that can be used for the visualization of NIIMS parcel data, along with spatial analysis.

The use of geographic information systems (GIS) enables the program to map field data, organize and analyze it, and assist with informed decision making. System administrators have access to system data and system audit logs to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Data may be shared with other DOI bureaus/offices that participate in proceedings or that have an interest in proceedings, for example the DOI Office of the Solicitor or the Office of Hearings and Appeals. Summary transaction data is updated in the FBMS, which is the Department-wide financial management system.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

To the Department of the Treasury as required by the Debt Collection Improvement Act (DCIA) to recover debts owed to the United States.

To a consumer reporting agency if the disclosure requirements of the Debt Collection Act, as outlined at 31 U.S.C. § 3711(e)(1), have been met.

Other disclosures may be made to external entities as outlined in the routine uses in INTERIOR/BIA-34, NIIMS SORN, which may be viewed on the DOI website at https://www.doi.gov/privacy/sorn.

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

To a Tribe operating a specific irrigation project under a Self-Determination contract under the Indian Self-Determination and Education Assistance Act, (Pub. L. 638, 25 U.S.C. section 450l). Shared information is limited to the specific project the tribe is operating.

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

Information may be shared with contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support and as authorized pursuant to the routine uses contained in INTERIOR/BIA-34, NIIMS SORN.

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

To owners of land on which Indian irrigation projects are constructed, operated, and maintained (including individual Indian and non-Indians and private sector parties (businesses)) to verify receipt of their payment. To realty and title companies to validate land ownership and billing information.

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.*

Individuals can decline to complete the Water Request form. Individuals and organizations voluntarily provide information when initiating services. Provision of minimal information for servicing accounts, such as TIN, is required by 25 C.F.R. 171.530 – 171.540 to obtain benefit.

☐ 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 (PAS): *Describe each applicable format.*

The PAS provides detailed information on the authority and purpose of collecting PII, how PII is used and with whom the PII is shared, the applicable routine uses under the INTERIOR/BIA-34, NIIMS SORN, and the voluntary nature of the collection, as well as impacts for not providing information.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this PIA, use of PAS on forms, and the published INTERIOR/BIA-34, NIIMS SORN, 78 FR 7804 (February 4, 2013), modification published at 86 FR 50156 (September 7, 2021). More information about the Department's privacy program including compliance documents and how individuals submit a request for agency records pertaining to them is available at DOI's Privacy Act Request website at https://www.doi.gov/privacy/privacy-act-requests.https://www.doi.gov/privacy/privacy-act-requests

A warning banner that provides details on expected uses of the system and privacy policies must be acknowledged before users can access the NIIMS functions.

☒ Other: *Describe each applicable format.*

Statement Pursuant to the Debt Collection Improvement Act of 1996 (Public Law 104-134), individuals are required to furnish BIA their TIN. The TIN required is the SSN, Employer ID Number (EIN), Internal Revenue Service (IRS) individual TIN or other TIN assigned to the individual or business named. If the agency collecting this information is required to file information with IRS identifying you, then you are required to furnish our office your TIN pursuant to Treasury Regulation §301.6109-1(b). If you do not have a TIN, then you are required to obtain one. Failure to provide this information, or the provision of incorrect information, may result in a $50 fine per document filed with the IRS (Treasury Regulation §301.6721).

☐ None

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

Records in NIIMS are primarily retrieved by name or customer identification number through ad-hoc and scheduled management reports.

I. Will reports be produced on individuals?

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

Authorized users have access to produce the following reports:

- Mailing addresses report – used for mailers.
- TIN report – lists customers who have or have not provided a valid TIN required by DCIA.

- Bankruptcy report – used for review of the status of bankruptcy proceedings.
- Deceased report – used for review of probate claims.
- Wrong address/ returned mail report – used to review and update non-current addresses.
- Statement of account – used to provide customers with an account balance.
- Customer mini-ledger – used to review all customer transactions.
- Detailed reports on receivables listing debtors, and outstanding bills with or without aging information – used as backup for continuity of operations (COOP).
- Lease listings including lessee information, used as backup for COOP.
- Ownership reports – displays owners of irrigable land, used as backup for COOP.
- Land reports including ownership – used as backup for COOP.
- Bill listings and exceptions – documents generated bills and billing exceptions.
- Demand letter listings and exceptions – documents generated demand letters and exceptions.
- Journal Voucher Numbers including information about the user that posted them, used to review entries and authorization.
- Security report showing users and access levels – used to review user access levels and authorization.
- Schedules of Collections showing payments received with details, documents collections and deposits.
- Collections listing all payments received within the reporting period – documents all collections.
- Delinquent bills eligible for referral to Treasury – used for review of bills to be referred.
- Bills referred to Treasury – reports on bills referred to Treasury.
- Bills returned from Treasury – reports on bills returned from Treasury.
- Bills recalled from Treasury – reports on bills recalled from Treasury.
- Bills exempt from referral to Treasury – used to prepare the Treasury Report on Receivables (TROR).
- Treasury collections – used in preparation of the TROR.
- Status report listing bills at Treasury – used for review of bills at Treasury.
- Bills under appeal – used for review of bills under appeal.
- Waivers with customer information – used for review of waivers.

Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. Audit logs capture account creation, modification, disabling, and termination; logon date and time, number of failed login attempts, files accessed, user actions or changes to records. Audit logs also collect information on system users such as username. System administrators and the information system owner have access to these 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 collected directly from individuals is presumed to be accurate at the time of submission and can update their information at any time to ensure it remains accurate. Billing information, such as names and addresses of owners and lessees of irrigable land, is based on legal documents

obtained from or verifiable with county clerk and recorder's offices, courts and DOI systems such as the Trust Asset and Accounting Management System (TAAMS), which may include name, addresses, TIN, Tribal Enrollment ID, land ownership and lease information, date of death, date of birth.

Users are responsible for ensuring the accuracy of the data associated with their user accounts. Data is checked for accuracy during the account creation process.

If an individual believes their records are not accurate, they can request corrections or the removal of material from the record by writing to the System Manager identified in the INTERIOR/BIA-34 SORN or by contacting the IA Associate Privacy Officer (APO). Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR part 2, subpart K.

B. How will data be checked for completeness?

Data collected directly from individuals must be complete at the time of submission and individuals can update their information at any time to ensure it is complete. The system contains required fields and validation controls to ensure completeness of data. For example, the TIN field in NIIMS requires numeric-only input.

Data is checked for completeness during the account creation process. Users are responsible for ensuring the completeness of the data associated with their user accounts.

If an individual believes their records are not complete, they can request corrections or the removal of material from the record by writing to the System Manager identified in the INTERIOR/BIA-34 SORN or by contacting the IA APO. Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR part 2, subpart K.

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

It is the responsibility of each Customer to ensure currency of the information provided. Individuals can update their information at any time to ensure it remains current. Billing and debt collection procedures require current information often provided by Customers as outdated addresses result in returned mail and billing disputes. Project offices cross-check information by soliciting updates from BIA Realty Offices, TAAMS, county offices, and a variety of other sources. The U.S. Treasury Cross Systems Next Generation system communicates TIN corrections as they encounter errors and resolve them.

User account information is provided directly by the user during account creation and can be updated by the user. Users are responsible for the accuracy of their records.

If an individual believes their records are not current, they can request corrections or the removal of material from the record by writing to the System Manager identified in the INTERIOR/BIA-34 SORN or by contacting the IA APO. Access procedures and requirements are outlined in the DOI Privacy Act regulations at 43 CFR part 2, subpart K.

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

Records are covered by IA Records Schedule (IARS) Records Series 4900 – Irrigation and Power and have been scheduled as permanent records under the National Archives and Records Administration (NARA) Job No. N1-075-04-006, approved November 21, 2003. Records are maintained in the office of records for a maximum of five years or when no longer needed for current business operations. The records are then retired to the American Indian Records Repository (AIRR) which is a Federal Records Center (FRC). Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the DOI and NARA.

Information Technology records are maintained under the Departmental Records Schedule (DRS) 1.4A Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer-term justification of the office's activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cutoff. Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version of upon termination of the system and destroyed three 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?

IA maintains records in accordance with the applicable DRS and IARS approved by NARA. Data dispositions follow NARA guidelines and approved record schedules for transfer, pre-accession, and accession to NARA. These activities comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and the Bureau of Trust Funds Administration, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of IA's records retention schedule. System administrators dispose of DOI records by shredding or pulping for paper records and degaussing or erasing for electronic records in accordance with NARA Guidelines, Departmental policy, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, Guidelines for Media Sanitization.

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 the privacy of individuals due to the sensitive PII contained in NIIMS. NIIMS 5.0 will undergo a formal Assessment and Authorization and is anticipating the issuance of an authority to operate in accordance with the FISMA and NIST standards. NIIMS is rated as a FISMA moderate system due to the type and sensitivity of data and requires security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, requires physical, technical, and administrative controls to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud,

misuse of credit, and exposure of sensitive information. Only authorized personnel with proper credentials can access the records in the system. DOI requires MFA for network and system access. System access is based on least privilege access and role-based access controls.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Only authorized personnel with proper credentials can access the records in the system. DOI requires multi-factor authentication for network and system access. System access is based on least privilege access, role-based access controls and the "need-to-know." Access control lists were created and segmented, users cannot view information for other users unless specifically authorized. BIA manages user accounts using the Bison System Access Management (BSAM) system to manage access. BSAM is the DOI-wide authoritative source for all identities and the primary solution for Identity Lifecycle Management (ILM). BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor onboards and until they depart DOI. BSAM is used to establish, activate, modify, review, and disable user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; 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 is reported to IT Security. Annually, employees, complete privacy training which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure they understand their responsibility to protect privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. Physical, technical, and administrative controls are in place and other security mechanism have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Data is encrypted during transmission and at rest. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that NIIMS may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained to provide a service or perform official functions. Authorized personnel with access to the system are instructed to collect the minimum amount of information needed to perform official functions for which the system was designed and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official functions. Employees complete privacy training which includes topics on the collection and unauthorized disclosure of information. Users are advised not to share sensitive data with individuals not authorized access and to review applicable system of records notice before sharing information.

Employees are aware information may only be disclosed to an external agency or third party if there is informed written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and "need-to-know" factors, based on the "least privilege" principle. Access restrictions to data and various parts of the system's functionality is role-based and requires supervisory approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. NIIMS meets BIA's information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. Data is collected directly from the customer through their application for water service and are responsible for ensuring the data provided is current. As published in the BIA-34 SORN, 43 CFR Part 2, Subpart K, an individual can request records the system may contain and if the individual believes the records are inaccurate can request corrections or the removal of material from the record as authorized 43 CFR Part 2, Subpart K, by writing to the System Manager identified in the SORN.

There may be a risk associated with the collection of information from other DOI systems. This risk mitigated as NIIMS 5.0 interfaces with other information systems via an encrypted, secure file transfer protocol.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The Division of Water and Power is responsible for managing and disposing of BIA records in NIIMS as the information owner. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. Division of Water and Power ensures only records needed to support its program, Tribes, and Tribal members is maintained. Division of Water and Power maintains the records for a maximum of five years or when no longer needed for current business operations, at which time they are transferred to the AIRR, a FRC for permanent safekeeping in accordance with retention schedules approved by NARA under Job Code N1-075-04-006, approved November 21, 2003. NIIMS system usage records are covered by the DRS 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by the NARA. These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off. Information collected and stored within NIIMS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not have adequate notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and through the published INTERIOR/BIA-34, National Irrigation Information Management System (NIIMS), 78 FR 7804 (February 4, 2013), modification published 86 FR 50158 (September 7, 2021), which may be viewed at: https://www.doi.gov/privacy/sorn. Additionally, PAS are part of the Water Request forms. The PIA, SORN, and PAS provide a detailed description of system source data elements and how an individual's PII is used.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. NIIMS 5.0 is hosted and administered within a DOI-approved and Federal Risk and Authorization Management Program (FedRAMP) certified hosting center. The cloud service provider will implement protections, controls and access restrictions as required to maintain the necessary FedRAMP Authorization to Operate (ATO). The provider will be required to submit to additional security accreditation to attain the DOI ATO to ensure the vendor's system handles and stores sensitive information in accordance with Federal and DOI privacy and security standards.

In addition to the risk mitigation actions described above, the BIA maintains an audit trail of activity sufficiently enough to reconstruct security relevant events. The BIA 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. Access to the DOI Network requires MFA. Users are granted authorized access to perform their official duties, and such privileges comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST SP 800-53. DOI employees must take Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness, Records Management, Section 508 Compliance, Controlled Unclassified Information (CUI), Paperwork Reduction Act (PRA), and Forms Compliance before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

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 use of the system and data collected is relevant and necessary to the purpose for which NIIMS was designed and supports the IA mission and to ensure compliance with 25 CFR 171, Irrigation Operations and Maintenance.

☐ 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. NIIMS is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable 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?

Users are only given access to data based on the "least privilege" principle combined with a "need-to-know" to complete assigned duties. BIA manages user accounts using the BSAM system. BSAM is the DOI-wide authoritative source for all identities and the primary solution for ILM. BSAM supports ILM requirements by providing a standard set of enterprise workflows that manage DOI identities from the time a new employee or contractor onboards and depart the DOI. BSAM is used to establish, activate, modify, review, disable user accounts. Federal

employee access requires supervisor approval. Contract officer representatives determine the level of access for contractors, which is approved by the information owner. Tribes who have contracted or compacted a government trust function may submit requests for access for tribal members working on a program, which must be approved by the program manager.

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.

Contractors are required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The privacy terms and conditions and the following Privacy Act contract clauses were included in the contract.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.224-3, Privacy Act Training (Jan 2017)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

☐ 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 purpose of NIIMS is not to monitor individuals, however user actions and use of the system is monitored to meet DOI security policies. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system.

☐ No

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

The NIIMS system is not intended to monitor individuals. However, the system has the functionality to audit user activity. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Firewalls and network security configurations are also built into the architecture of the

system and NIST SP 800-53, and other DOI policies are fully implemented to prevent unauthorized monitoring.

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

NIIMS can audit the usage activity within the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, and other DOI policies are fully implemented to prevent unauthorized monitoring. System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. System Administrators assign User roles based on the principle of 'least privilege' and perform due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to NIIMS Rules of Behavior. Users must complete annual IMT Awareness Training, which includes Privacy Awareness, Records Management, Section 508 Compliance, CUI, PRA, and Forms Compliance before being granted access to DOI information and information systems, and annually thereafter.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The NIIMS audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

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:* Multi-Factor Authentication

(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 Deputy Associate Chief Information Officer serves as the Information System Owner (ISO) for NIIMS 5.0. The ISO, Information System Security Officer (ISSO), and authorized bureau/office system managers are responsible for oversight and management of security and privacy controls and the protection of IA information processed and stored by NIIMS 5.0. The ISO and 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 by IA. The ISO is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, 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 IA APO.

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 NIIMS 5.0 ISO and ISSO are responsible for daily operational oversight and management of the system's security and privacy controls, 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 ISO, the ISSO and any authorized users are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC within one hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in coordination with the IA APO.