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.

Name of Project: NPS Water Rights Docket Files (WRD)

Bureau/Office: National Park Service/Natural Resource Stewardship & Science (NRSS) Directorate, Water Resources Division
Date: July 29, 2022
Point of Contact:
Name: Felix Uribe
Email: nps_privacy@nps.gov
Phone: (202) 354-6925
Address: 12201 Sunrise Valley Drive, MS 242, Reston, VA 20192

Section 1. General System Information

A. Is a full PIA required?

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

☐ No

B. What is the purpose of the system?

The National Park Service (NPS) Water Rights Docket Files (WRD) system stores documentation for water rights/water uses in park units. Project acquisition involved digital scanning, indexing, and archiving of 55,000 pages of documentation stored in over 1400 analog files associated with 177 park units.

This digital version of the NPS WRD files allow relocation of the original paper files to an offsite disaster-proof storage facility and facilitates for broader use of the information stored in the docket files. New paper documentation is incorporated into the system on a periodic basis. The system is currently used by NPS field staff, Washington DC Area Support Office, Water Resources Division staff, and by legal counsel in the Department of the Interior (DOI) Office of the Solicitor (SOL) to complete various work functions and tasks.

Documentation stored in the system includes legal water right filings and related correspondence transmitted between NPS and state agencies, intra-agency correspondence, legal opinions by SOL, history of development and acquisition of water rights by NPS, technical specifications of water supply systems and allowable rates of water use under state permits, NPS water use reporting to state agencies and other supporting hydrologic data, maps, and photos.

The source water documents and information are publicly accessible from states' databases available to the public and may contain names and addresses of Federal, state, or other government agencies and their personnel, water right holder names, and location of point of diversion for the use of water.

In summary, the system promotes better use of supporting documentation that outlines when, where, and how water has historically been used, or is currently used, at park units.

C. What is the legal authority?

- National Park Service Organic Act (54 U.S.C. 100101(a) et seq.)
- National Park Service General Authorities Act of 1970 (54 U.S.C. 100101(b) et seq.)
- National Parks Omnibus Management Act of 1998 (54 U.S.C. 100701 et seq.)
- Open, Public, Electronic, and Necessary Government Data Act (i.e., OPEN Government Data Act) which is Section 201 of the Foundations for Evidence-Based Policymaking Act of 2018 (P.L. 115-435)

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

E. Is this information system registered in CSAM?

☒ Yes
Water Rights Docket System Security and Privacy Plan
UII: 010-000000567

☐ 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	Describe
None			

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

☒ Yes
A new INTERIOR/NPS-36, Water Rights Docket, SORN is being developed to cover the water rights application and associated documents or records.

DOI Active Directory credentials are covered under: INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) (March 12, 2007, 72 FR 11040); modification published September 7, 2021, 86 FR 50156.

DOI SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☐ No

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

☐ Yes

☒ No

Information is collected from public records and is not collected directly from members of the public.

Section 2. Summary of System Data

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

☒ Name
☒ Mailing/Home Address
☒ Other

Documentation stored in the system includes legal water right filings and related correspondence transmitted between NPS and state agencies, intra-agency correspondence, legal opinions by SOL, history of development and acquisition of water rights by NPS, technical specifications of water supply systems and allowable rates of water use under state permits, NPS water use reporting to state agencies and other supporting hydrologic data, maps, and photos. These documents may include contact information on deed holders, water right or land transfer applicants, NPS personnel, or personnel of other agencies, as well as, docket title or number, permit number, application number, or parcel identifiers, domestic uses, name, official email address, and official address.

The source water documents and information are publicly accessible from states' databases that are available to the public and may contain names and addresses of other governmental agencies and their personnel, water right holder names, and location of point of diversion for the use of water.

PII for NPS employees and contractors is required for authentication, account management and logging purposes. NPS users use their government issued Personal Identity Verification (PIV) card authenticated through the Enterprise Active Directory (AD).

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

PII may be collected from electronic documents or records submitted to NPS from the above organizations or those available in the public domain.

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

Documents received via fax, email, or website are output as paper documents. Paper documentation is also retained in paper format in secured file cabinets. Physical controls are implemented and documented for controlling access to the paper documents.

Telephone interviews conducted by NPS with other agencies to clarify docket content may be documented and associated with the docket.

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

PII collected is used to support natural resources research. For each water use, a water right docket is created containing relevant documentation that establishes the date of first use, the amount used (both instantaneous and annual amounts), the purpose or need, the source of water, the point of diversion and place of use, the continuous use of the right, and any changes to the amounts, purposes, or source of water over time.

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

☒ Within the Bureau/Office

Information is shared with named users in the Water Resources Division who are system users entering and reviewing the information in the WRD system. Dockets suitable for release are exported to and made available through the Integrated Resource Management Applications (IRMA) data store subsystem. The IRMA PIA is available at https://www.doi.gov/sites/doi.gov/files/irma-pia.pdf.

☐ Other Bureaus/Offices

☐ Other Federal Agencies

☐ Tribal, State or Local Agencies

☒ Contractor
NPS contractors are involved with the installation and configuration of the software, application and database support, and management of the servers and other network infrastructure. Contractor and cooperator staff are required to undergo background checks as defined by NPS policy and procedures. Contractor and cooperator staff access will be restricted to data on a need-to-know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in the System Security Plan and Privacy Plan. This maintenance is critical to protecting the system and the PII contained within the system.

☐ Other Third-Party Sources

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

☐ Yes

☒ No
The data is already part of the public record that was obtained from Federal, State, Local, and Tribal governments. These government agencies are responsible for providing the opportunity for individuals to decline to provide the information or consent to the use of their PII as required by their laws and policies.

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

☐ Privacy Act Statement

☒ Privacy Notice
Notice is provided through publication of this Privacy Impact Assessment and will also be provided through the proposed and published SORNs. This information is collected from other governmental sources that collect the data in support of records to maintain information in support of water resources. These governmental sources are responsible for providing notice to individuals as required by their laws and policies.

☐ Other

☐ None

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

The data is already part of a public record and obtained from governmental sources. Depending upon the water resource in question, various records are collected through digital records such as land deeds or water right transfers. Data is retrieved by docket title or number, permit number, application number, or parcel identifiers, domestic uses, and last name.

I. Will reports be produced on individuals?

☐ Yes

☒ No

Section 3. Attributes of System Data

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

Public records from other agencies are assumed to be verified for accuracy by the provider agency. As documents are added to a docket, the NPS supervisor conducts quality control checks to ensure accuracy of information entered.

NPS user information is collected form the individual during onboarding or generated by NPS or DOI as DOI records such as email address, name and/or User Principal Name (UPN) during operational activities. Non-DOI users are not approved for access to the system.

B. How will data be checked for completeness?

As documents are added to a docket, the NPS supervisor conducts quality control checks to ensure completeness of information entered.

WRD users are responsible for ensuring the completeness of the data associated with their user accountants and content posted into WRD. Users are responsible for ensuring the completeness of the data they submit when requesting DOI AD access. PII used in the account creation is initially provided by the individual during onboarding. During the account creation process, the user account administrator will validate the account request against DOI AD information, and any incomplete data will result in an error preventing

creation of the account. Incorrect data prevents user authentication and may be identified by administrators when reviewing activity reports.

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

WRD periodically reviews dockets to identify changed, missing, or out of date information. WRD is working to develop a more robust reporting of changed docket information.

DOI User information such as name, user-id and/or UPN is obtained from the DOI AD. Changes made within AD are tracked within the WRD system.

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 WRD are retained in accordance with the NPS Records Schedule, Resource Management and Lands (Item 1), which has been approved by the National Archives and Records Administration (NARA) (Job No. N1-79-0801). The disposition of Cultural and Natural Resource Management Program and Planning records, including applications for permits, permits and investigator annual reports, is permanent. Periodic transfer of special media and electronic records along with any finding aids or descriptive information (including linkage to the original file) and related documentation by calendar year are transmitted to NARA when 3 years old. Final transfer of all permanent records to NARA occurs 15 years after closure. Digital records will be transferred according to NARA standards applicable at the time.

The disposition of records with short-term operational value and not considered essential for ongoing management of land, cultural and natural resources is temporary, including account management records. These operational records are destroyed/deleted 15 years after closure. The disposition for routine housekeeping and supporting documentation is temporary and records are destroyed/deleted 3 years after closure. Detailed disposition procedures and processes are defined and published to internal system administration staff within the WRD technical reference manuals.

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

The approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

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 are privacy risks to individuals due to the PII collected, and WRD is rated as a FISMA Moderate system. Information access and retrieval through electronic means follows defined application security roles and permissions to ensure proper distribution and disclosure of information guided by the principle of least privilege to minimize the risk of improper information disclosure. The protection and maintenance of information for recovery and backup purposes is done following NPS data center policy and process for backup and retention of information. Disposition of all information are guided by the NPS records retention schedules for systems that manage information.

There are privacy risks related to unauthorized access to the system or data, inappropriate use, disclosure of information to unauthorized recipients, or that information may be used outside the scope of the purpose for which it was collected. NPS personnel with access to recorded material and digital evidence will be subject to strict NPS policy, bureau policy, and privacy control standards. Only authorized personnel with proper credentials can access the records in the system. NPS requires two-factor authentication for network access. System access is based on least privilege access and role-based access controls. NPS employees and contractors must take Information Management and Technology (IMT) awareness training, which includes privacy, security, records management, Section 508, Paperwork Reduction Act, and Controlled Unclassified Information, both prior to the granting of access 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. Disclosure of sensitive information or PII to unauthorized recipients, failure to protect PII, mishandling of PII or misuse of PII may result in criminal, civil, and administrative penalties. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Transport Layer Security (TLS) technology is employed to protect information in transit using both server authentication and data encryption. Device level encryption have been deployed to encrypt data at rest. Other security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

There is a risk that user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes or use of data. Federal employees and contractors

are required to take annual IMTLT awareness training as well as role-based privacy training (RBPT) and role-based security training (RBST) where applicable and sign the NPS Rules of Behavior prior to accessing the system. 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.

There is a risk that erroneous information may be collected from Federal, State, Local, and Tribal governments or from public records. This risk is mitigated by quality control check for accuracy and completeness.

There is a risk that information in the system will be maintained longer than necessary to achieve the agency's mission or may be improperly disposed or destroyed. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Detailed procedures and automated scripts for data disposal/destruction will be developed and secured under change management. Contingency plans and procedures will be defined to ensure the ability to recover in the event of improper data disposal.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used, or how to seek access to or correction of their records. This risk is mitigated by the publication of this PIA and the SORNs. Docket information is collected from governmental agencies and is not collected from individuals. The DOI Privacy Program website also contains DOI and NPS privacy officials' contact information and provides guidance to individuals on how to submit requests or complaints under the Privacy Act.

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
Information in WRD is used to store documentation for water rights/water uses in park units in a central location and improve NPS resource management utilizing best-available information.

☐ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

☐ Yes

☒ 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.

☐ Yes, processes are being consolidated.

☒ 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

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

Access will be restricted for all users. Each user will be assigned permissions, groups of permissions may be used to define a user's role. The permissions will determine what function the user may execute in the system and define what records the user can create, read, edit, or delete.

System management staff may on occasion be required to view PII in the performance of their duties for troubleshooting or system maintenance purposes. Employee or contractor staff with privileged accounts will be subject to routine auditing to ensure compliance with policies and procedures for managing data confidentiality and integrity.

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 responsible for designing, developing, and maintaining the system, and in accordance with DOI policies, Privacy Act contract clauses are included in all contractor agreements in accordance with and subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations.

Contractor employees interfacing with the system and/or related data or providing services, administration or management are required to sign nondisclosure agreements as a contingent part of their employment. Contractor employees are also required to sign the DOI's Rules of Behavior and complete security and privacy training prior to accessing a DOI computer system or network. IMT awareness, RBPT, and RBST training must be completed on an annual basis as an employment requirement. Contractor and/or contractor personnel are prohibited from divulging or releasing data or information developed or obtained in performance of their services, until made public by the Government, except to authorized Government personnel. Contractors are also subject to Federal Acquisitions Regulations (FAR) with regard to sensitive data; however, no sensitive PII is collected or managed by the WRD system.

☐ 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

☒ No

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

☐ Yes

☒ No

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

The system is not intended to monitor individuals. However, audit logs are used to monitor and protect against unauthorized access, changes or use of data. The audit logs contain information on username, IP address, time/date, login status, etc.

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

All system administrators are required to take annual RBST, RBPT, and IMT Awareness Training.

Separation of duties, permission restrictions, and audit controls are implemented to prevent unauthorized monitoring. Procedures are published for granting accounts, and privileged accounts are routinely audited for compliance.

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

(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

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 Chief, Water Rights Branch serves as the WRD System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in WRD. The System Owner and System Privacy Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within WRD, in consultation with NPS and DOI Privacy Officials.

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 WRD Information System Owner and WRD Information System Security Officer are responsible for daily operational oversight and management of the security and privacy controls, for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The WRD Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure

of PII is reported to DOI-CIRC and appropriate NPS and DOI officials in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the NPS Associate Privacy Officer.

System administrators and contractors are required to report any potential loss or compromise to the Information System Owner and Information System Security Officer.