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: Dive Management System (DMS)
Bureau/Office: National Park Service, National Dive Program
Date: July 15, 2022
Point of Contact:
Name: Felix Uribe
Title: NPS Associate Privacy Officer
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) Dive Management System (DMS) is a web-based system that supports diving programs/operations throughout NPS. NPS conducts dive operations for maintenance, scientific, and public safety purposes. The DMS hosts diver records, dive logs, safe practices worksheets, dive project plans, equipment inventory and maintenance records, and diver and program management tools for Park Dive Officers (PDOs), Regional Dive Officers (RDOs), the NPS National Dive Officer (DSO), and the

NPS National Dive Control Board (NDCB). This system is fundamental to the operation and oversight of a safe and effective NPS diving program by tracking diver training, qualification, and adherence to Federal policy requirements. Dive log records document the amount of effort expended to accomplish underwater tasks for NPS purposes and diver requirements, track diving activity, including any accidents, to ensure safety of divers.

All NPS employees and volunteers diving in the Park Service are trained at experience levels ranging from novice to expert. Information is collected on the diver's experience and training, preexisting certification to use different modes of diving equipment, different breathing gases, and performance in different diving environments and tasks. Information is also documented and tracked regarding training received while working for the Park Service and administrative requirements for working as a diver for NPS. All of this is necessary to ensure employee health and safety, that the individual is qualified and authorized to perform the tasks assigned to meet the needs of the Park Service, and to protect the agency by documenting that safety practices and policies are being met. Dive log and dive plan information is collected so that task efforts can be measured, plans can be evaluated for safety, and that the work will be performed by qualified/authorized individuals to ensure safety trends and injury rates can be identified and evaluated. A centralized, web-based data management system allows program managers to audit the effectiveness of training and operational efforts remotely and standardizes record keeping practices for diving within the Park Service.

C. What is the legal authority?

Occupational Safety and Health Administration, 29 CFR 1910.401 subpart T, Commercial Diving Operation

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
System Security and Privacy Plan (SSP): NPS Dive Management System Security and Privacy Plan
UII Code: 010-00002872

☐ 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

Employee records are covered under OPM/GOVT-1, General Personnel Records, 77 FR 79694 (December 11, 2012); modification published 80 FR 74815 (November 30, 2015)

Volunteer records are covered under INTERIOR/DOI-05, Interior Volunteer Services File System, 66 FR 28536 (May 23, 2001), modification published 86 FR 50156 (September 7, 2021).

DOI Personal Identify Verification (PIV) credentials for accessing the system are covered under 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).

These SORNs may be viewed on the DOI SORN website https://www.doi.gov/privacy/sorn.

☐ No

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

☐ Yes

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Birth Date
☒ Education Information
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Other

General employment classification – Dive is a collateral duty for almost all individuals in the Park Service. General Schedule (GS), Wage Grade (WG), Law Enforcement (LE), or Volunteers In Parks (VIP) tags are recorded so that reports can be generated on the general areas of employment where divers are originating from.

Year of birth, month of birth or month prior/after birth information is necessary so the system can track and calculate the need for required medical examinations. Actual date of birth is not recorded.

The system generates a unique identifier for each diver registered and each park and/or RDO. The unique identifier is assigned by the system when the individual is entered into the system. This number is specific to the DMS and has no other application beyond the system. It is used to link data associated with the individual throughout the various tables in the database.

Information associated with required/recurring training is collected so that requirements can be audited, training courses scheduled, and dive qualifications/authorizations tracked and adjusted per dive policy requirements. This information includes the type of training, dates, and expiration dates for determining when to retrain.

Assigned equipment lists (optional, individual program specific) are collected so that equipment inventory and maintenance can be tracked including life control equipment assigned to individuals and items requiring periodic testing requirements.

Dive log data collects dive minimum requirements per DOI policy and dives executed by an individual annually. Dives are reviewed for policy requirements and to generate reports related to individual efforts, including diver identifier, dive location, dates, depth, time, task performed, dive classification, dive mode used, dive tables or computers used, and dive buddy.

Diver authorization data includes Letters of Reciprocity (LOR) and Verifications of Training (VOT) for coordination with other bureaus and agencies. LORs are used to attest to diver qualifications/authorizations and are exchanged between agencies. VOTs are generated and exchanged when the individual moves between agencies or requests a record for their personal records. These documents may include diver name, email address, qualifications and expiration dates, diver authorizations, and NPS name, official title, and signature of the PDO, RDO, or DSO.

Dive plans submitted per policy for review/approval include diver names and reference to their qualifications/authorizations.

User email address and password are collected for access control. NPS staff must authenticate through Active Directory to the NPS network to access DMS. NDCB members may access the system to view reports only. Divers, PDO, RDO, and DSO access to information is restricted to their own information and/or the information required for their program responsibilities.

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

Verification of training letters are provided by other entities including Federal or state government agencies, academia, or private entities.

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

Boat dive logs are recorded on paper in the field and manually entered in the system website. The diver and the appropriate dive officer are responsible for securing the paper record for the relevant time period for the dive classification and executing disposal of the paper record in accordance with the applicable records schedule.

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

PII collected will be used to ensure safety and qualification of divers participating in Dive Program events or incidents.

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

☒ Within the Bureau/Office

The data is shared between NPS Dive Management Program, NPS park and office units, and the NDCB. Data is used to determine diver qualifications and experience for diver project and task assignments, for auditing of training and operation effectiveness, for tracking policy compliance, and safety and performance measures.

☒ Other Bureaus/Offices

LORs are used to attest to diver qualifications/authorizations and are exchanged between bureaus. VOTs are generated and exchanged when the individual moves between bureaus or requests a record for their personal records. LORs and VOTs allow individual divers to present evidence of qualification and experience gained in NPS to other bureaus for the individual to participate in other bureaus' dive programs.

☒ Other Federal Agencies

LORs are used to attest to diver qualifications/authorizations and are exchanged between agencies. VOTs are generated and exchanged when the individual moves between agencies or requests a record for their personal records. LORs and VOTs allow individual divers to present evidence of qualification and experience gained in NPS to other agencies for the individual to participate in other agencies' dive programs.

☒ Tribal, State or Local Agencies

LORs are used to attest to diver qualifications/authorizations and are exchanged between agencies. VOTs are generated and exchanged when the individual moves between agencies or requests a record for their personal records. LORs and VOTs allow individual divers to present evidence of qualification and experience gained in NPS to other agencies for the individual to participate in other agencies' dive programs.

☒ Contractor

Contractors are responsible for the operations and maintenance of the software platform. Contractors need access to the platform to provide support and maintenance for the application that hosts PII but will not have access to the actual PII data. This maintenance is critical to protecting the system and the PII contained within the system.

☒ Other Third-Party Sources

Upon request of an individual diver, an LOR or VOT may be provided to a third-party, such as a university, consulting firm or other entity identified at the discretion of the diver. LORs are used to attest to diver qualifications/authorizations and are exchanged between entities. VOTs are generated and exchanged when the individual moves between other entities or requests a record for their personal records. LORs and VOTs allow individual divers to present evidence of qualification and experience gained in NPS to other entities for the individual to participate in other entities' dive programs.

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

☒ Yes

Individuals voluntarily provide information when applying to participate in the Dive Program. An individual may decline to share their information by not completing the application, however, they may not be able to participate in the Dive Program or associated training and related opportunities.

☐ No

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

☒ Privacy Act Statement

A link to a Privacy Act Statement will be provided on each DMS screen when collecting PII.

☒ Privacy Notice

Notice will be provided through publication of this PIA and the applicable published SORNs.

☒ Other

Users will be provided with a privacy and security warning banner when accessing the system, which informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system..

☐ None

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

Information in the system may be retrieved by name and the system assigned unique identifier. Summary reports can be retrieved by training requirements and expiration dates, diver status, fiscal year, date range, or location.

I. Will reports be produced on individuals?

☒ Yes

Information requested is necessary for the management of the NPS Dive Program in accordance with policy requirements in 29 CFR 1910 Subpart T, DOI 485 DM 27, NPS Director's Order 4 and NPS Reference Manual/Field Manual 4.

Eligibility reports will be generated to determine eligibility of individuals for a diving collateral duty or volunteer position based on number of hours completed. This report will only contain an individual's system generated unique identifier, name, and qualification or authorization status. These reports will only be accessible to specific users based on roles assigned.

LORs are used to attest to diver qualifications/authorizations and are exchanged between agencies. VOTs are generated and exchanged when the individual moves between agencies or requests a record for their personal records.

☐ No

Section 3. Attributes of System Data

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

PII information is collected directly from individuals and is assumed to be accurate. While performing data entry using the website, data validations will ensure that the correct type of information is being entered. To the extent practicable, data entry validations are implemented to ensure data integrity. Federal agency staff may periodically verify that the information provided is accurate and complete and may request the individual update or correct pertinent data.

B. How will data be checked for completeness?

PII information is collected directly from individuals, and individuals are responsible for ensuring all necessary information is complete. When data entry is performed using the website, users will not be able to save the information until all required fields have been completed. To the extent practicable, data entry validations are implemented to ensure data integrity. Federal agency staff may verify information provided for accuracy and completeness.

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

Users are responsible for updating and providing new information at a set interval of time within the DMS. A formal full review is conducted annually by NPS park and/or regional diving officers and the NPS NDCB. The system stores and displays the last modified date as well as last modified user information.

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

DMS records are maintained in accordance with the NPS Records Schedule, Category 2: Protection and Safety (Item 2B), which has been approved by the National Archives and Records Administration NARA) (Job No. Nl-79-08-2). The disposition for the dive personnel records is temporary and records are destroyed/deleted 25 years after closure (after the diver is separated from the program).

Certain other documents in the system (e.g., dive logs, ad hoc reports, etc.) are more resource related and should be maintained in accordance with the NPS Records Schedule, Category 1: Resource Management and Land Records (Item 1C), which was also approved by NARA (Job No. N1-79-08-1). The disposition for records of short-term operational value is temporary and records are destroyed/deleted 15 years after closure (end of fiscal year in which the dive occurred).

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

For temporary records, approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and the 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 types of PII collected. Multiple controls have been implemented to mitigate and substantially lower privacy risks. Data entry is only performed through the DMS web application and will be protected by encryption to safeguard the data both while in transit and at rest. Web applications follow 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. Disposition of all information are guided by the NPS Records retention schedules.

A formal Assessment and Authorization for issuance of an authority to operate will be conducted in accordance with the Federal Information Security Modernization Act (FISMA), and the system will be rated as moderate, requiring management, operational, and technical controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. As part of continuous monitoring, continual auditing will occur to identify and respond to potential impacts to PII information.

There are privacy risks related to hosting, processing, and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls, many of which will be referenced in the completed System Security and Privacy Plan. 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, the system incorporates the use of role-based permission to give access to limited sets of PII. 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 server authentication. Device level encryption has been deployed to encrypt data at rest on laptop computers. 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 of data interception in transit between the user’s web browser and the application server. This risk is mitigated by encryption of data in transit.

There is a risk that user PII may be inappropriately used for an unauthorized purpose 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 security, privacy, records management, Section 508, Paperwork Reduction Act, and Controlled Unclassified Information, as well as privacy and security role-based training 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 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 information including PII may be output from users’ web browsers and improperly secured or disposed. All PII information including reports is access-controlled, and only NPS staff with the appropriate need-to-know will be given access. DOI mandates that all Federal employees and contractors complete initial and annual information security and privacy training. The resulting high awareness provides an enhanced level of assurance on the life cycle management of the PII data. Physical media including printed reports is manually collected and secured following the program-defined process for ensuring chain of custody and appropriate safeguards until the physical media is disposed of by shredding or pulping for paper media or erasing or degaussing for electronic physical media.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA, applicable SORNs, and Privacy Act Statements within the system. NPS will request that Partner organizations provide a Privacy Act Statement to participants when collecting their information, as appropriate.

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

Federal agencies are provided authority to maintain and collect PII in support of the agency's mission. Information on individuals is necessary to support safety in the dive program. This information is both relevant and necessary as it is used to provide safety management of dive projects. The data will also help track various eligibility criteria for the divers. Diving in the Park Service is a collateral duty for a majority of NPS divers. All employees and volunteers diving in the Park Service have training at experience levels ranging from novice to expert. Information is collected on the diver's experience and training, preexisting certification to use different modes of diving equipment, different breathing gases, and performance in different diving environments and tasks. Information is also documented and tracked regarding training received while working for the Park Service and administrative requirements for working as a diver for NPS. All of this is necessary to ensure employee health and safety that the individual is qualified and authorized to perform the tasks assigned to meet the needs of the Park Service, and to protect the agency by documenting that safety practices and policies are being met. Dive log and dive plan information is collected so that task efforts can be measured, plans can be evaluated for safety, and that the work will be performed by qualified/authorized individuals to ensure safety trends and injury rates can be identified and evaluated. A centralized, web-based data management system allows program managers to audit the effectiveness of training and operational efforts remotely and standardizes record keeping practices for diving within the Park Service.

☐ 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?

New data is not created or derived by the system.

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 a role functions) and permissions. The role will determine what function the user may execute in the system while the permissions will define what records the user can create, read, edit, or delete.

Select PII data fields will be encrypted and only available on a need-to-know basis. For example, certain demographic information will be viewable by the users who have permissions to add/update the information and not by other users or by other partner organizations. This type of data may be used for analytical and performance reporting on an agency, bureau or unit and is not necessary for viewing on the individual level.

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 are required to sign the DOI's Rules of Behavior and complete security and privacy training prior to accessing a DOI computer system or network. Information security and privacy awareness and role-based privacy and security 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) regarding sensitive data.

NPS contractor staff are required to undergo background checks as defined by NPS policy and procedures. Contractor 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 published procedures.

☐ 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

DMS is not intended for monitoring users, however, the system does identify and monitor user activities within the system through audit logs. Audit logs automatically collect and store information about create/update/delete activities performed by users to support data integrity and incident response support.

Monitoring will primarily target users with privileged accounts, such as system administrators who can change configuration settings or escalate access permissions or roles; however, login history is recorded for all users, and field history tracking is recorded for select data fields, including some PII data elements.

☐ No

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

Record change history tracking will be applied to sensitive data elements or elements that, if subject to unauthorized change, could present a risk to identity authentication or to the mission or business process. These elements include dive log entries and user id changes.

A minimum number of system administrators will be able to access platform configuration settings, and all platform configuration settings will be monitored for changes. All privileged accounts will be monitored and routinely audited.

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

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, Office of Risk Management serves as the DMS Information 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 the DMS. The Information System Owner and Information System Security 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 DMS, 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 DMS Information System Owner and DMS 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 DMS 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.