U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our Privacy Office Support Request Page. For further guidance, consult the DOI PIA Guide.

System Information

System or Project Name:	Damage Assessment and Restoration Tracking System
System or Project Acronym:	DARTS
Bureau or Office:	Office of Restoration and Damage Assessment
Date submitted for review:	June 18, 2026
System Operational Status:	Development

Point of Contact

Name:	Jamie Huang
Title:	Privacy Officer
Office:	Department Privacy Office
Phone:	(202) 208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: System Overview

1. What triggered this PIA? (Check one)

☐ New System
☒ Significant Modification
☐ New Electronic Collection
☐ Other: Describe below

DARTS is undergoing a significant modernization that moves the system from the existing USGS-hosted environment to the DOI OCIO Cloud Hosting Solution AWS environment and substantially changes the application architecture, hosting boundary, authentication, interfaces, and system capabilities, including an embedded AI-assisted search capability.

2. What is the purpose of the system or project?

The Damage Assessment and Restoration Tracking System (DARTS) is a web-based case management and tracking system used by the Department of the Interior's Natural Resource Damage Assessment and Restoration

(NRDAR) Program to manage information throughout the lifecycle of natural resource damage cases.

DARTS supports case development, damage assessment, settlement, fund request processing, restoration planning and implementation, monitoring, and case closure. The system enables authorized users to manage and track case records, documents, funding information, restoration activities, case status, and related legal, scientific, economic, financial, and administrative information.

DARTS also supports collaboration among DOI personnel and authorized Federal, State, and Tribal co-trustees involved in NRDAR activities and provides public access to approved case information, maps, case pages, and documents that have been reviewed and cleared for public release.

DARTS includes search and reporting capabilities to help users locate relevant case, document, funding, and restoration information and support efficient management of NRDAR program activities.

3. Is the system registered in BisonGRC?

☐ Yes: If applicable What is the project's UII code?
☒ No: Explain why this is not either done or required.

DARTS is undergoing modernization and transition from the legacy USGS-hosted environment to the DOI OCIO Cloud Hosting Solution AWS environment. Development of the modernized application is currently underway, and the new OCIO authorization boundary has not yet completed the BisonGRC/RMF authorization process.

BisonGRC registration, system-boundary documentation, and Authority to Operate activities for the modernized DARTS environment are being coordinated with OCIO as part of the cloud migration.

The architecture and safeguards described in this PIA for the modernized AWS environment represent the target DARTS production environment and must align with the final authorized configuration before operational deployment..

4. What legal authorities authorize the collection and use of data in this system or project?

The Natural Resource Damage Assessment and Restoration (NRDAR) Program is primarily authorized by three Federal statutes and their implementing regulations:

- Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), 42 U.S.C. §§ 9601 et seq.
- Oil Pollution Act of 1990 (OPA), 33 U.S.C. §§ 2701 et seq.
- Clean Water Act (CWA), 33 U.S.C. §§ 1251 et seq.

These authorities allow DOI and other natural resource trustees to assess injuries to natural resources resulting from hazardous substance releases or oil discharges, recover damages from responsible parties, and use those recoveries to restore injured resources. The NRDAR Program also operates under the National Oil and Hazardous Substances Pollution Contingency Plan, 40 CFR Part 300, which supports coordinated Federal response and restoration activities.

DARTS supports these authorities by tracking NRDAR cases throughout their lifecycle, including case initiation,

assessment activities, settlement documentation, fund requests, restoration projects, monitoring, and case closure. DARTS also supports public transparency by making approved case information and documents available for public review.

Additional authorities supporting NRDAR funding and transfers include the Department of the Interior and Related Agencies Appropriation Act, 1992 (P.L. 102-154) and the Department of the Interior and Related Agencies Appropriation Act, 1996 (P.L. 104-134).

For additional information on NRDAR authorities, guidance, and policy, see DOI's Restoration Program Authorities, Guidance, and Policy Library.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

☐ Yes: If yes, list the applicable citations below.
☒ No

DARTS NRDAR case records are organized and retrieved by system-generated Case ID rather than by an identifier assigned to an individual.

DARTS also maintains user-account, authorization, access, role, and audit information associated with identifiable authorized users. Applicable DOI logical-access records are covered by INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), 72 FR 11040 (March 12, 2007), as subsequently modified.

Authentication records maintained by GSA as part of Login.gov are covered by GSA/TTS-1, Login.gov, 89 FR 41436 (May 13, 2024).

DARTS does not rely on those access-management SORNs as coverage for the underlying NRDAR case records.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

☐ Yes
☒ No

DARTS supports information collection and workflow activities associated with the NRDAR program under OMB Control Number 1091-0002, which the program identifies as applicable to the information collection implemented through DARTS. The responsible Information Collection Clearance Officer maintains the PRA determination and clearance applicable to the collection.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

None

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

☒ Name (full, first or last)	☐ Home telephone number	☐ Employment or resume info
☒ Aliases/nickname	☐ Personal Email	☐ Full or Truncated SSN
☐ Driver's license	☐ Mailing or home address	☐ Physical characteristics
☐ Citizenship	☐ Religious preference	☐ Biometrics/facial recognition
☐ Legal Status	☐ Mother's maiden name	☐ Vehicle information
☐ Sex	☐ Marital status	☐ Passport information
☐ Race or ethnicity	☐ Spouse Information	☐ Travel information
☐ Date of birth	☐ Child or family information	☐ Parent's name
☐ Place of birth	☐ Emergency contact info	☐ Credit card number
☐ Personal cell phone number	☐ Financial information	☐ Nationality
☒ Username / user ID / acct ID	☒ IP address / network ID	☒ Device ID / online ID
☐ Geolocation / GPS / location	☐ Photos / video / audio	☐ Health / medical information
☐ Tribal or other ID number	☐ Education information	☐ Disability Information
☐ Criminal / disciplinary info	☐ Military records	☒ Other: Describe below

DARTS primarily maintains business and system-access information concerning authorized Federal, State, Tribal, local, contractor, and other approved users. This information includes name, username/account identifier, organization, official title or role, trustee affiliation, system role and access level, Login.gov account linkage, authentication/session information, audit information, and business contact information used for NRDAR case coordination and system administration.

DARTS also maintains the names and business contact information of case team members, fund-request submitters, document submitters, and other officials participating in NRDAR activities.

NRDAR case documents and correspondence maintained in DARTS may contain limited PII associated with the underlying official case record. DARTS does not routinely collect Social Security numbers, home addresses, dates of birth, personal financial information, or medical information as structured DARTS data fields**.**

2. What is the source for the PII collected? Check all that apply.

☒ Individual	☒ DOI Records
☒ Federal Agency	☐ Third Party Records
☒ Tribal Agency	☒ State Agency
☒ Local Agency	☐ Other: *Describe Below*

DARTS receives user identity and account information from authorized individuals and approved identity and access-management services. DOI users authenticate using DOI enterprise credentials. Authorized external co-trustee users authenticate through Login.gov. DARTS maintains the user profile, organization or trustee affiliation, assigned role, access level, and audit information necessary to administer access within DARTS.

Login.gov authentication records remain maintained by GSA under its Login.gov privacy documentation and are not DARTS-owned authentication records.

3. How will the information be collected? Check all that apply.

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☒ Website
☐ Fax
☐ Telephone Interview
☐ Shared Between Systems: *Describe*
☒ Other: *Describe*

DARTS collects user and case information through the DARTS web application and receives authentication assertions through the approved identity services described above.

The modernized DARTS architecture uses AWS components to enforce application-level roles and permissions within the authorized DARTS environment. The final PIA and security documentation will use consistent terminology to distinguish enterprise identity authentication from DARTS application authorization.

DARTS does not currently have an operational interface with ECOSphere. ORDA and FWS are evaluating a one-way DARTS-to-ECOSphere integration intended to reduce duplicate data entry. That proposed integration is not part of the current operational data flow.

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

The PII is being collected to log into DARTS either through PIV card for DOI users or Login.gov, assigned to the user roles in DARTS, and be assigned to cases. This information is not publicly displayed.

Note: A geolocation is being recorded for any project that is requesting to proceed through the NRDAR process. The geolocation is that of a public resource, such as river, swamplands, etc. and is not associated with an individual. This location is collected to associate the case with a DOI region and to be able to display the location on both internal and public-facing maps.

5. How does this project limit the collection and use of PII to only what is necessary?

Name and username data is the minimum required to perform DARTS functions and assign user roles and responsibilities to individuals in the system. Most DARTS users are federal employees, and a subset are from state, local, or tribal organizations. With the use of PIV card access or Login.gov authentication, this minimizes the collection of PII to only the information needed to gain access to the system**.**

Section 3: Data Sharing and Individual Rights

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

☒ **Within the Bureau/Office:** Describe how the data will be used below.
☒ **Tribal, State or Local Agencies:** Describe how the data will be used below.
☒ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☒ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☐ **Other Third-Party Sources:** Describe how the data will be used below.

Within DOI: Authorized users from DOI offices and bureaus may access DARTS information according to their

assigned NRDAR role, case responsibilities, information classification, and need-to-know.

Other Federal agencies: Authorized Federal co-trustee personnel may access NRDAR case information assigned to their role and case responsibilities.

Tribal, State, and local governments: Authorized co-trustee users from Tribal, State, and local governmental entities may access information associated with the NRDAR matters on which they are authorized to participate.

Contractors: Contractors supporting DARTS design, development, maintenance, or operations may access information necessary to perform assigned duties. Contractor access is governed by assigned role, need-to-know, contractual requirements, and applicable security and privacy controls.

DARTS uses role and information-access designations to distinguish DOI-only, internal/co-trustee, and public information .

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☐ Yes
☒ No

The system does not have an MOA/MOU however, the program has various MOA/MOUs with State, Tribal, and other Federal Agencies for cooperation as co-trustees for these NRDAR cases. Since the inception of this system over 10 years ago, DOI was the only user for about 6 years. OS only recently added a mirrored feature for co-trustees to request their funds from the fund. With the new system modernization, the office wanted to increase the transparency with the co-trustees by providing access to the same system internally to facilitate better cooperation on NRDAR cases through the process to follow other Federal Agencies' lead (i.e. NOAA-DIVER).

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*
☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Name and system-generated username is required for the system to function and display the party representing the state, local, or tribal Agency. Providing business contact information is voluntary; however, individuals who decline to provide the information required for account provisioning cannot access DARTS.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

☐ Privacy Act Statement:
☒ Privacy Notice:
☐ Other: *Describe Below*
☐ None: *Example - law enforcement cases.*

DARTS provides a system privacy notice to authorized users at login describing the purpose of the collection, account and access information maintained by DARTS, how the information is used, whether information required for account provisioning is mandatory or voluntary, and applicable privacy contacts.

DOI logical-access records are addressed under INTERIOR/DOI-47, and Login.gov authentication records maintained by GSA are addressed under GSA/TTS-1. The DARTS notice distinguishes DARTS-maintained user information from authentication information maintained by the external identity provider.

Public transparency regarding the broader DARTS system and NRDAR information practices is also provided through this PIA.

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

Not retrieved by personal identifier other than Case ID, which is a sequence number (ie: Case # 427) that has no meaning outside of DARTS. The cases are about the destruction of a natural resource, rather than about an individual.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

There are user role reports containing DOI user's names and their associated roles. These are reviewed by regional staff, national level staff, and Administrators for accuracy on a quarterly basis to verify the correct roles are still associated with the correct staff members. DARTS sends emails for various functions including requesting signatures for case funding applications, concurrence with Authorized Official Nominations, Acceptance of Case Closure, and Acceptance of an Authorized Official Nomination. It is important that we receive these signatures from the correct Regional Directors from the various DOI Bureaus**.**

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

The system shall use Login.gov to authenticate external users attempting to log in. So it's up to the user to provide accurate authentication data.

Accuracy of assessment and damage dat**a** is verified through in person and aerial assessments conducted by the federal government, partners, or contractors throughout the NRDAR case process (i.e. Authorized Official Designation, settlement, and restoration). Since many of our cases gain local news traction or are listed on other official Federal Agency Websites (i.e. National Oceanic and Atmospheric Administration, U.S. Environmental Protection Agency), DOI case team staff and DARTS Administrators will review data when entered for accuracy and compare the information to make sure it is consistent. Data will be displayed from FBMS for financial case information use.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

DARTS operational records are currently unscheduled. Until applicable NARA-approved disposition authority is established and confirmed, DARTS Federal records will be preserved and will not be destroyed based solely on a proposed schedule, system configuration, or business-use determination.

ORDA Records Management is coordinating the appropriate disposition authority for final NRDAR case records and other DARTS record series. Final case records are expected to have long-term or permanent value, but the controlling schedule and disposition instructions will be identified based on the approved NARA authority.

Drafts, working materials, reference copies, system records, account and audit records, and other DARTS information will be disposed of only under an applicable NARA-approved disposition authority.

DARTS also retains AI interaction and evaluation information, including prompts, model context, outputs, traces, model/prompt/agent versions, and evaluation records. ORDA Records Management will determine the recordkeeping status, applicable disposition authority, and retention implementation for these materials.

Applicable legal holds, litigation, investigations, audits, FOIA/document-production obligations, and other preservation requirements suspend normal disposition when required.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

The system shall conduct an automated comparison of the latitude/longitude coordinates with the state and region selected in the system to ensure the project site is where the user indicates it is; no AI is involved. Damage assessments are conducted by DOI, co-trustees, or contractors to validate assessment information. Cases that are funded through the Case Funding Application process within the program have the Technical Support Group reviewing cases and the provided supporting documentation for review of accuracy and approvals for funding. Information submitted through the Transaction requests for tracking the withdrawal or return of funds for cooperative assessments, recovered costs, CFA funds, and restoration are reviewed by ORDA trained staff to review accuracy. The Budget Officers for the NRDAR Fund, within ORDA, continues the review with the information in DARTS prior to execution of funds movements from FBMS. DARTS does not move funds in FBMS. There will be a connection to FBMS to display the totals for financial accounts associated with cases for case teams to have better accounting for their finances throughout the NRDAR process. These totals and changes in totals will match the reflected transaction requests within DARTS which contain the supporting documentation for the transaction. All changes made by DARTS administrators are verified with the DOI and Co-trustees assigned to the case to ensure accuracy of data and the reflected changes.

3. Does the project include logging capabilities to record and monitor access to PII?

☒ Yes
☐ No

Yes, the system logs whenever an administrator makes changes to usernames or roles, which is the only PII

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

Account and access risk: DARTS maintains identifiable user, role, access, trustee-affiliation, and audit information. There is a risk that this information could be accessed, retained, or used beyond its authorized administrative and NRDAR coordination purposes. Role-based access, account reviews, authentication controls, audit logging, and removal of access when no longer required mitigate this risk.

Case-document PII risk: NRDAR case documents and correspondence may contain PII beyond the structured business-contact information maintained in user profiles. Internal and public-release controls are used to limit access and prevent inadvertent disclosure.

AI processing risk: The embedded AI search capability can access DARTS case information within the requesting user's permissions and generates outputs and detailed interaction traces. Risks include inaccurate responses, inappropriate retrieval, prompt injection, unintended exposure of restricted case content, excessive retention of prompts or outputs, and use of AI-generated information without appropriate human validation.

DARTS mitigates these risks through permission-bounded read-only retrieval, human review, content and prompt-injection safeguards, evaluation testing, auditability, access controls, and restrictions on the AI capability to approved user roles.

Public-release risk: DARTS provides public access to approved NRDAR content. Information designated for public release undergoes the program's established review process before publication to reduce the risk of releasing PII, privileged information, or other restricted content.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

☒ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☐ No

The system generates new data through the Case Funding Applications and the Transaction Requests. The Case Funding Applications data is created through the budget form calculating their final request using their submit case costs minus their carryovers reported. The applications are reviewed by the Technical Support Group (TSG) who does vote on funding cases based on the strength of the case, cost analysis of the assessment, and if the funds are need at that time. The data is verified through System Admins initial review of data entry, 2 review periods of the TSG and verification from the case team through communication with System Admins and the TSG that their answers are correct. All answers are maintained as DOI only and are labeled as Attorney-Client Privileged documentation not to be shared with anyone outside the case team, ORDA, and the TSG.

Transaction requests calculate new data fields for summed totals of the request for all entry from the supporting documentation for the requested or return of funds. These are manually reviewed by ORDA staff for accuracy to the supporting documents and the funding available in FBMS.

All data that is generated for DOI only consumption, will be labelled as such and hidden from the Co-Trustee

User Role. Information pertaining to total funding that is withdrawn for cases is considered public once the case is in restoration and is able to be accessed and viewed on the NRDAR Status Report website**.** Funding decisions are made with the aid of this new data; the data is never the only source of decision to fund a restoration/repair site.

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

☐ Yes: *Provide explanation below*
☒ No

No, the new data will be stored in the case record, not the individual records.

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

☐ Yes: *Provide explanation below*
☒ No

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

All new data generated by the system is reviewed by ORDA (System Administrators and Budget Officers) and the TSG for accuracy and relevance**.**

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

☒ Yes
☐ No, *Proceed to Section 7.*

2. How are models validated for fairness, accuracy, and transparency?

DARTS does not train or fine-tune its own foundation model. DOI validates the DARTS AI capability at the application and use-case level to determine whether outputs are sufficiently accurate, relevant, safe, and transparent for the authorized search function.

Validation includes a curated test set, deterministic checks of tool selection and arguments, required-content and refusal tests, evaluation of answer quality, regression testing when the model, prompt, or tools change, and human review of results.

Foundation-model provider controls are part of the overall risk environment but do not replace DOI's responsibility to validate the DARTS implementation for its intended use.

3. Are individuals notified of AI-based decisions that affect them?

☐ Yes
☒ No

N/A The models are just used to search for cases, documents, and projects, and has no influence on individuals.

4. Are safeguards in place to prevent bias or unintended consequences?

☒ Yes
☐ No

AI prompts, retrieved context, outputs, and associated interaction traces may contain DARTS case information. Access to retained AI interaction records is restricted to personnel with an authorized administrative, security, evaluation, or program need. These records are protected under the same information-access restrictions applicable to the underlying DARTS information and are subject to DOI records and preservation requirements.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

☒ Yes
☐ No

Changes to the foundation-model version, system prompt, retrieval tools, permissions, or material data flows trigger re-evaluation before promotion to the operational DARTS environment. Human review remains required because successful technical evaluation does not make AI-generated content authoritative case information.

6. Is federated learning used for privacy-preserving model training?

☐ Yes
☒ No

The system does not train/fine-tune new model but use pre-trained foundation model (Claude Sonnet) through Amazon Bedrock**.**

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe below*

DARTS access is restricted through authenticated identity and application-level role-based authorization.

DOI users authenticate through the approved DOI enterprise identity service, and authorized external co-trustee users authenticate through Login.gov. Within DARTS, application roles and permissions determine which cases,

documents, functions, and information classifications each user may access.

Administrative privileges are restricted to authorized system administrators. Contractors and developers receive only the access required to perform assigned development, maintenance, or operational duties.

2. What data protection policies apply to cloud-based PII storage?

The modernized DARTS system is designed to operate within the DOI OCIO Cloud Hosting Solution AWS environment under the applicable DOI authorization boundary. PII is protected through DOI cloud-security requirements and applicable NIST SP 800-53 Rev. 5 security and privacy controls.

Protections described for the modernized environment include encryption of information in transit and at rest, private network segmentation, role-based access, multifactor authentication, audit logging, threat detection, security monitoring, restricted administrative access, and controls governing access to the DARTS data tier.

The final cloud configuration, inherited controls, authorized services, AI capability, and permitted data types must match the approved DARTS authorization package before production use.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

PII is stored in a dedicated database tier within isolated private subnets (no internet egress; AWS-bound traffic restricted to VPC endpoints). Access is governed by Amazon Cognito user pools, which handle authentication, MFA, and group/role-based authorization. Cognito controls *who may access* the system; detection of *anomalous or unauthorized behavior* is handled by a separate, layered monitoring stack:

- Audit logging (system of record). AWS CloudTrail captures every control-plane and data-plane API call — including S3 data events and Cognito sign-in/token events — recording principal, action, timestamp, and source IP. VPC Flow Logs on the isolated DB subnets record every connection attempt to the data tier, so any access from an unexpected source or any attempted lateral movement is logged. Database-level audit logs capture the queries executed against the PII store itself.
- Threat detection. Amazon GuardDuty continuously analyzes CloudTrail, VPC Flow Logs, and DNS telemetry to detect anomalies — credential misuse, atypical API patterns, connections to known-malicious endpoints, and unusual data-access volumes indicative of exfiltration. Because the DB subnets have no normal egress path, any anomalous outbound activity is high-signal and surfaced immediately.
- Alerting and response. GuardDuty findings and high-risk CloudTrail patterns (e.g., disabled logging, bulk reads, new credential creation) trigger CloudWatch Alarms / EventBridge rules, which publish to an SNS topic routed to the security on-call. This closes the loop from detection to notification in near-real-time.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.
☐ No

DARTS performs user-linked security, administrative, and system-activity monitoring to protect system integrity, investigate unauthorized access, and maintain accountability.

Monitoring may include authentication events, source IP information, access and role changes, administrative activity, system and database events, and AI interaction/audit information.

Access to monitoring information is restricted to authorized security, system-administration, audit, evaluation, and program personnel based on role and need-to-know. Monitoring information is used for authorized security, administration, compliance, evaluation, and incident-response purposes.

5. Will contractors be involved in the following project activities? Check all that apply.

☒ Design
☒ Development
☒ Maintenance

Contractors are required to complete background checks, complete role-based security training and sign non-disclosure agreements.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

☐ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks
☐ Identification Badges
☐ Safes
☐ Combination Lock
☐ Other: *Describe Below*

Technical Controls

☐ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Other: *Describe Below*
☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

Administrative Controls

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☐ Other: *Describe Below*
☒ Methods to Ensure Only Authorized Personnel Have Access
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Records and Privacy Training
☐ Regular Monitoring of Users' Security Practices

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

Individuals seeking access to Privacy Act records maintained about them in connection with DARTS may submit a Privacy Act request in accordance with DOI Privacy Act regulations and the access procedures applicable to the relevant system of records.

DOI logical-access records associated with DARTS are addressed under INTERIOR/DOI-47. Authentication records maintained by Login.gov are maintained by GSA under GSA/TTS-1 and are subject to GSA's applicable Privacy Act procedures.

Privacy Act access procedures are separate from public access to NRDAR case information and from FOIA requests for agency records.

8. What processes are in place for individuals to access their information?

Individuals seeking access to Privacy Act records maintained about them in connection with DARTS may submit a Privacy Act request in accordance with DOI Privacy Act regulations and the access procedures applicable to the relevant system of records.

DOI logical-access records associated with DARTS are addressed under INTERIOR/DOI-47. Authentication records maintained by Login.gov are maintained by GSA under GSA/TTS-1 and are subject to GSA's applicable Privacy Act procedures.

Privacy Act access procedures are separate from public access to NRDAR case information and from FOIA requests for agency records.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may request amendment or correction of Privacy Act records about themselves in accordance with DOI Privacy Act regulations and the procedures applicable to the relevant system of records.

Routine corrections to DARTS business-profile or role information may also be addressed through authorized system-administration processes. Administrative correction does not replace applicable Privacy Act amendment rights.

10. 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?

Program Manager/System Owner/Information System Security Officer/Authorized User – Reports privacy breach or inappropriate disclosure of Privacy Act records to ISSO
ISSO - Immediately reports the breach to the DOI Computer Incident Response Center (DOI-CIRC) at (703) 648-5655 or DOICIRC@ios.doi.gov

Submissions are routed to the DOI Privacy Office Breach Response Team for triage and coordination. The DOI Privacy Office leads breach triage, risk assessment, reporting to oversight authorities, and stakeholder coordination.
Email: privacy@ios.doi.gov
Phone: 202-208-1605

All DOI personnel and contractors with access to DARTS data are required to report the loss, compromise, unauthorized disclosure, or unauthorized access of PII to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI Privacy Officer within one hour of discovery, in accordance with the DOI Privacy Breach Response Plan. This layered accountability structure ensures that both prevention and timely reporting are embedded into system operations.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

In the event of a privacy breach involving DARTS, DOI will follow the procedures outlined in the **DOI Privacy Breach Response Plan**:

1. **Immediate Reporting** – Any suspected or confirmed breach must be reported within **one hour** of discovery to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI Privacy Officer.
2. **Containment and Mitigation** – The ISSO and DOI-CIRC work to secure affected systems, revoke compromised credentials, and prevent further data loss.
3. **Risk Assessment** – The Privacy Officer and breach response team assess the nature and scope of the breach, the sensitivity of the compromised PII, and the potential risk to affected individuals.
4. **Notification** – If required, affected individuals will be notified without unreasonable delay, consistent with OMB M-17-12 and DOI policy, providing:
    - A description of the incident
    - The type of information involved
    - Steps individuals can take to protect themselves
    - DOI contact information for questions and assistance
5. **Oversight Reporting** – DOI will report to OMB, Congress, DHS, and other required oversight bodies when thresholds for major incidents are met.
6. **Remediation and Prevention** – The system team will implement additional controls, update procedures, and retrain personnel to prevent recurrence.

These steps ensure a coordinated, timely, and compliant response to mitigate harm to individuals and uphold DOI's legal obligations.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

DARTS will be reviewed annually through the applicable DOI Privacy Threshold Analysis process and whenever a

material change to system functionality, cloud architecture, user population, PII, interfaces, external sharing, public-release capability, AI functionality, model or provider configuration, records practices, or operational use may affect privacy risk.

This PIA will be updated when a material change makes the public assessment inaccurate or incomplete. When review confirms that no material privacy change has occurred and the existing PIA remains accurate, it may be reaffirmed in accordance with DOI privacy procedures.