U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Document Review & Production (DR&P)
Bureau/Office: Office of the Chief Information Officer (OCIO)
Date: April 3, 2023
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

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

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

Document Review & Production (DR&P) is a cloud-based solution that enables the Department of the Interior (DOI) personnel to collect, review, redact, and produce documentation as part of various document production requests, including Freedom of Information Act (FOIA) requests,

Congressional Oversight requests, litigation, Administrative Records preparation, and possibly investigations. The solution is provided by Everlaw as a Software-as-a-Service (SaaS), which is FedRAMP authorized and hosted by the Amazon Web Services (AWS) cloud service provider. DR&P serves as an online document repository that is used to filter through all documents that are potentially responsive to requests. DR&P is an enterprise platform that is segregated for the different program areas to ensure only authorized individuals have access to the appropriate documents. The Office of the Chief Information Officer (OCIO) manages DR&P and DOI bureaus and offices are users of the tool.

Previously, the Enterprise eArchive System (EES), Enterprise Content System (ECS), Early Case Assessment (ECA), and Advanced Early Case Assessment (AECA) within the eMail Enterprise Records Document Management System (eERDMS) provided the framework for storing, accessing, and managing the Department's records. In particular, the ECA and AECA worked to manage collections created within ECS to support OMB Circular A-130 areas, e-Discovery, and internal investigations. The replacement of ECA and AECA with DR&P enables DOI staff to more efficiently and consistently respond to document production requests received from Congressional inquiries, the courts, or via FOIA requests.

In all document requests received, OCIO personnel will identify document custodians that possess the information being requested. These document custodians may be any DOI personnel that have documents related to the specific request and are the source for providing the information being reviewed. Any office can create a document request with appropriate authorization. The DOI Office of the Solicitor (SOL), in most instances, may assist in developing the effective search terms. Users requesting discovery and collection documents must complete and submit the DI-4003, Departmental Audit Request Form, with the appropriate approvals. The DI-4003 form is used to submit the automated request and help develop the search terms for eDiscovery requests. The DI-4003 form must also contain the reason for the search request as documented on the form. All requests are sent to an internal OCIO email address for processing. If the appropriate approvals are not on the form, it is sent back for correction. OCIO personnel, including document custodians, will conduct the searches requested and compile the results. Their individual searches of the documents are conducted across all DOI platforms, including Microsoft 365 (M365) (Teams and SharePoint), eERDMS, etc. A listing of all inquiries being processed is documented in the SharePoint Discovery and Collections Dashboard, which is maintained by the OCIO Information Management Branch, and is visible to all DOI staff. This is to allow requestors access to the progress of their inquiry. The output results of the inquiries themselves are loaded into the DR&P system to be reviewed, and any necessary redactions are added prior to being produced in response to FOIA, Congressional Oversight Request, litigation, etc.

DR&P receives the documents in numerous formats, including Microsoft Office documents, emails, PDFs, and other formats that are provided by DOI staff or directly extracted from DOI's M365 or eERDMS platforms. DR&P stores the search results in their native formats, which are reviewed by the document reviewer. The documents are loaded into the Everlaw review database tool and then indexed. This allows the documents to be searched, sorted, and organized to help document reviewers determine proposed redactions based on applicable laws. Once the

redactions are confirmed, they are permanently "burned" into a copy that can be exported for distribution to various external parties, as necessary.

Documents produced will be exported and retained in the Department's electronic repository for the appropriate records retention period, which may be distinct from the original retention period for the record. Results will be maintained in DR&P as business needs warrant for the inquiry. An administrator is designated over each inquiry type and will determine necessary steps for disposal of the documents once the inquiry is closed.

C. What is the legal authority?

- The Clinger-Cohen Act of 1996, 40 U.S.C. 1401
- 36 CFR 1220: Federal Records, General
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service*
- Presidential Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments*
- Presidential Memorandum, *Building a 21st Century Digital Government*

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

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

DR&P is registered in the DOI Governance, Risk, and Compliance system. The System Security and Privacy Plan is in development.

010-000002876 - OCIO - Infrastructure - Information Management and Compliance

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

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

☒ Yes: *List Privacy Act SORN Identifier(s)*

Records on FOIA requests are covered by INTERIOR/DOI-71, Electronic FOIA Tracking System and FOIA Case Files, 81 FR 33544 (May 26, 2016); modification published 86 FR 50156 (September 7, 2021). Litigation records are covered by INTERIOR/SOL-1, Litigation, Appeal and Case Files, 46 FR 12146 (February 12, 1981); modification published 86 FR 50156 (September 7, 2021). Archived data may be obtained from OS-10, Electronic Email Archive System (EEAS), 68 FR 4220 (January 28, 2003); modification published 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021). Due to the nature of DR&P as part of DOI's enterprise records management system and processing documents from numerous DOI systems, Congressional inquiries and requests for records production or investigation may be covered by Government-wide, Department-wide or bureau/office Privacy Act SORNs, which may be viewed on the DOI SORNs website at 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
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Biometrics
☒ Other Names Used
☒ Truncated SSN

☒ Legal Status
☒ Place of Birth
☒ Religious Preference
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Law Enforcement
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Race/Ethnicity
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Due to the nature of DR&P processing documents for different programs and missions, there may be numerous PII on the original documents that are reviewed.

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:

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:

Due to the nature of DR&P processing documents for different programs and missions, there may be numerous formats used to collect PII for the original documents that are reviewed.

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

DR&P is a cloud-based solution that enables DOI personnel to collect, review, redact, and produce documentation as part of various document production requests, including FOIA requests, Congressional Oversight requests, litigation, Administrative Records preparation, and possibly investigations. DR&P serves as an online document repository that is used to filter through all documents that are responsive to the requests. Where allowable by the governing laws (FOIA, Privacy Act, etc), PII is redacted from the documents prior to their release.

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

☒ Within the Bureau/Office:

The Departmental Records Officer within the OCIO Information Management Branch manages and maintains the DR&P system. Records maintained in DR&P are copies of documents pulled from other sources, which are used for document production purposes, such as Congressional Inquiries, Litigation Support, and FOIA, etc. The SOL, FOIA, and the Office of Congressional & Legislative Affairs (OCL) officials review document collections to determine what needs to be redacted and what is appropriate for release, depending on the specific request.

☒ Other Bureaus/Offices:

Records maintained in DR&P are copies of bureau/office documents pulled from other sources, which are used for document production purposes, such as Congressional Inquiries, Litigation Support, and FOIA, etc. The SOL, FOIA, and OCL officials review document collections to determine what needs to be redacted and what is appropriate for release, depending on the specific request.

☒ Other Federal Agencies:

Other Federal Agencies do not access DR&P directly. However, records maintained in DR&P are copies of documents pulled from other sources, which are used for document production purposes, such as Congressional Inquiries, Litigation Support, and FOIA, etc. DOI SOL, FOIA, and OCL officials review document collections to determine what needs to be redacted and what is appropriate for release, depending on the specific request. Information may be shared with other Federal agencies as authorized and required to meet legal and reporting requirements in accordance with the Privacy Act and applicable SORNs.

☒ Tribal, State or Local Agencies:

Tribal, State, or Local Agencies do not access DR&P directly. However, records maintained in DR&P are copies of documents pulled from other sources, which are used for document production purposes, such as Congressional Inquiries, Litigation Support, and FOIA, etc. DOI SOL, FOIA, and OCL officials review document collections to determine what needs to be redacted and what is appropriate for release, depending on the specific request. Information may be shared with other entities as authorized and required to meet legal and reporting requirements in accordance with the Privacy Act and applicable SORNs.

☒ Contractor:

Information may be shared with contractors who provide support for these program activities.

☒ Other Third-Party Sources:

Other Third-Party Sources do not access DR&P directly. However, records maintained in DR&P are copies of documents pulled from other sources, which are used for document production purposes, such as Congressional Inquiries, Litigation Support, and FOIA, etc. DOI SOL, FOIA, and OCL officials review document collections to determine what needs to be redacted and what is appropriate for release, depending on the specific request. Information may be shared with other entities as authorized and required to meet legal and reporting requirements in accordance with the Privacy Act and applicable SORNs.

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

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ No:

DR&P is a records query and collection system, and does not collect PII directly from the individual. Rather, the information is collected from various DOI systems and records, which do not provide individuals with an opportunity to decline to provide information in the records management process.

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

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice:

Notice is provided to individuals through the publication of this privacy impact assessment (PIA), related PIAs, and applicable SORNs published in the *Federal Register*.

☐ Other: *Describe each applicable format.*

☐ None

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

DR&P query records may be retrieved using various types of keyword searches or provided by document custodians. The search criteria used will depend on specific search needs but may include personal identifiers such as name and email address. Other personal identifiers may also be used, at the discretion of the individual performing the search. When retrieving data through automated searches all requests go through an audit request form process with management approvals that ensure the searches are within appropriate need and scope.

I. Will reports be produced on individuals?

☒ Yes:

Audit reports can be produced to review the actions of authorized system users to determine if their use of the DR&P system and the data has been in accordance with all rules and procedures for the system. Only users with elevated rights can run audit reports.

Statistical reports generated for system maintenance generally do not contain sensitive PII.

☐ No

Section 3. Attributes of System Data

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

DR&P enables DOI personnel to collect, review, redact, and produce documentation as part of various document production requests, including FOIA requests, Congressional Oversight requests, litigation, Administrative Records preparation, and possibly investigations. DR&P

serves as an online document repository that is used to filter through all documents that are potentially responsive to the requests. As such, it relies on the sourcing systems and processes to ensure that the information provided is accurate. Otherwise, documents captured in queries are intended to be duplicates of the originals and are not otherwise checked for accuracy.

B. How will data be checked for completeness?

DR&P enables DOI personnel to collect, review, redact, and produce documentation as part of various document production requests, including FOIA requests, Congressional Oversight requests, litigation, Administrative Records preparation, and possibly investigations. DR&P serves as an online document repository that is used to filter through all documents that are potentially responsive to the requests. As such, it relies on the sourcing systems and processes to ensure that the information provided is complete. Otherwise, documents captured in queries are intended to be duplicates of the originals and are not otherwise checked for completeness.

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

DR&P enables DOI personnel to collect, review, redact, and produce documentation as part of various document production requests, including FOIA requests, Congressional Oversight requests, litigation, Administrative Records preparation, and possibly investigations. DR&P serves as an online document repository that is used to filter through all documents that are possibly responsive to the requests. As such, it relies on the sourcing systems and processes to ensure that the information provided is current. Otherwise, documents captured in queries are intended to be duplicates of the originals and are not otherwise checked for currency. Since DR&P pulls data from various systems, including record keeping systems, by definition, some of the information retained in various components is historical and not current due to the requirements of the Federal Records Act.

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

Retention periods for records captured by DR&P vary according to agency needs and specific subject matter, and are retained in accordance with applicable Departmental Records Schedule (DRS) authorities as approved by the National Archives and Records Administration (NARA). Records retention periods may also be suspended by litigation holds, court orders, preservation notices, and similar issued by SOL, the DOI or Bureau Records Officer, and/or other authorized official.

Documents produced will be exported and retained in the Department's electronic repository for the appropriate records retention period, which may be distinct from the original retention period for the record. Search results will be maintained in DR&P as business needs warrant for the inquiry. An administrator is designated over each inquiry type and will determine necessary steps for disposal of the documents once the inquiry is closed. Records are destroyed when no longer needed.

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

DR&P does not have an automated retention functionality. Since DR&P is used for document production purposes, all records contained in these systems are considered copies of the original and need to be maintained for as long as the Congressional inquiry, FOIA request, litigation, or other oversight request remains active. Approved disposition methods include purging, degaussing, or erasing of 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 in the DR&P due to the volume and types of documents that are processed in response to FOIA requests, Congressional Oversight requests, litigation, Administrative Records preparation, and investigations. DR&P's primary privacy risks include unauthorized access, unauthorized disclosure, and misuse of the data in the system. These risks are addressed and mitigated through a variety of administrative and logical security controls. When retrieving data all requests go through an audit request form process with management approvals that ensure the searches are within appropriate need and scope or are documents provided directly by the records custodian.

User access is granted only to authorized individuals by system administrators, and users are granted access only to the data sets needed in order to perform their job duties. Only authorized users are provided access to DR&P using single sign-on and validated through the DOI Active Directory. Administrative access to DR&P is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In many cases, administrators can be granted adequate rights to fulfill their duties without being given access to data in the system. All user access policies and procedures are documents in the DR&P Account Administration Guide which is reviewed annually for necessary updates and signed off by the System Owner.

All users of DOI network resources, including contractors, must consent to DOI Rules of Behavior and take annual end-user security, privacy and records training in order to obtain access to any DOI network resource. DR&P administrators are also required to take security and privacy role-based training.

DR&P has a hierarchical administration consisting of Organizational Administrators, and multiple Database and Project Administrators who supervise administrators at the Department level, as well as DOI bureaus and offices. The DR&P Administrators are responsible for controlling and monitoring access to DR&P users who are given access to data for their Bureau or Office. DR&P Administrators and authorized employees are only granted access to documents and data in DR&P to the extent it is necessary for the performance of their job

duties. Access procedures are further described in the DR&P System Authorization and Accreditation (A&A) documentation and the system security and privacy plan.

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. In addition, firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to ensure system and data security. System administrators will review the activities of the users to ensure that the system is not improperly used, including for unauthorized monitoring.

Access is restricted to only those individuals authorized by System Administrators on a need-to-know basis in order to perform their job duties consistent with the purposes of the system. This includes limiting authorized individuals' access to selected repositories of documents and data within the system, such as the authorized individual's bureau or office. Limitations on access are maintained through role defined by the DR&P Administrators and validated upon user login and authentication. The audit logs for DR&P may be used to run reports on individual users' access to and actions within the system.

There is a risk that data from different sources may be aggregated and may provide more information about an individual. This data may become outdated or inaccurate. Mitigation occurs prior to document production. Records are disposed based upon the records management schedule.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. The provider will implement protections and controls to restrict access to unauthorized parties, as will be required to attain the necessary FedRAMP Authority to Operate (ATO). The provider will be required to submit security accreditation to attain the DOI ATO to ensure the vendor's system handles and stores sensitive information in accordance with Federal and DOI privacy and security standards.

There is a risk that individuals may not have adequate notice regarding the collection of information, the purposes for collection or how the information will be used. Notice is provided through the publication of this PIA, applicable SORNs, and related PIAs that apply to the original source documents.

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:

DR&P allows DOI to address program specific concerns such as producing documents for appropriate requests made outside of DOI that should be kept for legal and accountability purposes, achieving confidence in the authenticity and reliability of records, maintaining context to understand records properly, and controlling and planning for technological change that could make records inaccessible or incomprehensible.

☐ No

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

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*
☒ No

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

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable. DR&P enables DOI personnel to collect, review, redact, and produce documentation as part of various document production requests, including FOIA requests, Congressional Oversight requests, litigation, Administrative Records preparation, and possibly investigations. DR&P serves as an online document repository that is used to filter through all documents that are potentially responsive to the requests. Thus, DR&P does not derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated.

Access to information will be limited to those authorized individuals that have a need to know the data in order to perform official duties, including system administrators, authorized program personnel, and contractors based on least privileges.

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other:

Access to information will be limited to those authorized individuals that have a need to know the data in order to perform official duties, including system administrators, authorized program personnel, and contractors based on least privileges.

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

Access level restrictions, authentication, least privileges, and audit logs are used to ensure users have access only to the data they are authorized to view. Access is further governed by DOI IT security policy, including use of assigned passwords, limited access rules, various firewalls, and other protections put in place to ensure the integrity and protection of information. All DOI employees and contractor employees undergo initial and annual security, privacy and records management training, and sign DOI Rules of Behavior before being granted access to DOI networks and information.

DR&P has a hierarchical administration consisting of Organizational Administrators, and multiple Database and Project Administrators who supervise administrators at the Department level, as well as DOI bureaus and offices. DR&P Administrators are responsible for controlling and monitoring access of authorized records staff who are given access to data for their Bureau or Office. DR&P Administrators and authorized employees are only granted access to documents and data in DR&P to the extent it is necessary for the performance of their job duties. Access procedures are further described in the DR&P System Authorization and Accreditation (A&A) documentation and the system security and privacy plan.

Access is restricted to only those individuals authorized by DR&P Administrators on a need-to-know basis in order to perform their job duties consistent with the purposes of the system. This includes limiting authorized individuals' access to selected repositories of documents and data within the system, such as the authorized individual's bureau or office. Limitations on access are maintained through user login and authentication.

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. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors were involved with the design and configuration of the system and will be involved with the maintenance and operation of the system. Federal Acquisition Regulation (FAR) contract Clause 52.224-1, Privacy Act Notification (April 1984), FAR contract Clause 52.224-2, Privacy Act (April 1984), FAR contract Clause 52.239-1, Privacy or Security Safeguards (August 1996), FAR contract Clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (June 2016), FAR contract Clause 52.224-3, Privacy Training (January 2017), and 5 U.S.C. 552a are included by reference in the agreement with the contractor. The contract includes the terms and conditions for security, privacy, records, and controlled unclassified information, which are described in the DOI IT Baseline Compliance Contract Guidelines.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

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

☒ Yes.

DR&P is not intended to monitor individuals. However, the system has the ability to audit usage of the system, including reviewable data concerning logins, including login time, to protect against unauthorized access or actions within the system. Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. In addition, firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to ensure system and data security. System administrators will review the activities of the users to ensure that the system is not improperly used, including for unauthorized monitoring.

☐ No

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

DR&P is not intended to monitor individuals. However, the system has the ability to audit usage of the system, including use by authorized individuals and system administrators. This includes reviewable data concerning actions within the system, including username, date and time of day a user accessed the system, specific uniform resource locators (URLs) of component systems, search terms or parameters used to call data, user creation and deletion of files, user creation or deletion of user accounts, and changes to account privileges.

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

DR&P is administered by Department assigned users and a DOI contractor. The agreement with the contractor includes by reference FAR contract Clause 52.239-1, Privacy or Security Safeguards (Aug 1996). These regulations proscribe privacy protections including safeguards against unauthorized use of the data and unauthorized monitoring of individuals. Only authorized users will be able to access the system. In addition, all users must consent to the DOI Rules of Behavior and complete Cybersecurity, Privacy, and Records Management awareness training, as well as role-based privacy and security training before being granted access to the DOI network or any DOI system, and annually thereafter.

Access to DR&P must be approved by the system owner or designated representative before access can be granted. Audit logs are used to ensure individual user access and actions are authorized and within the scope of official duties, and the user traceability program can detect and report unauthorized attempts to access files outside the scope of a user's permissions.

The audit log feature, unique identification, authentication and password requirements, along with mandatory annual security, privacy and records management training requirements, help prevent unauthorized monitoring, as well as unauthorized access to data, browsing and misuse.

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. Cyber locks

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

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

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view. In addition, firewalls and network security arrangements are built into the architecture of the system and NIST guidelines and Departmental policies are implemented for system and data security. System administrators will monitor the activities of authorized users to ensure that the system is properly used.

Additionally, the audit trail features, unique identification, authentication and password requirements, and mandatory security, privacy and records management training requirement prevents unauthorized access to data, browsing and misuse.

All personnel must consent to DOI Rules of Behavior and complete annual mandatory security, privacy and records management training in order to receive and maintain access to the DOI network or systems.

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 DR&P Information System Owner and system administrators are responsible for protecting individual privacy and will ensure that only authorized DOI and contractor employees can access the system. The SOL, FOIA, and the OCL officials review document collections to determine what needs to be redacted and what is appropriate for release, depending on the specific request.

In addition, the Departmental Records Officer within the Principal Deputy CIO Division, Office of the Chief Information of Officer serves as the DR&P Information System Owner and the official responsible for oversight and management of the security and privacy controls for the information stored and processed in DR&P. The Information System Owner is responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies and for protecting the privacy rights of the public and employees, and addressing privacy complaints in coordination with 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 DR&P Information System Owner, Information System Security Officer, and System Administrators are responsible for ensuring the proper use of DR&P. Authorized users are also responsible for ensuring the proper use of DR&P in accordance with Federal laws and policies. The DR&P Information System Owner, Information System Security Officer and all authorized users are responsible for protecting individual privacy and reporting any potential compromise to DOI-CIRC, the Department's incident reporting portal, and DOI privacy officials in accordance with Federal policy and established DOI procedures. In accordance with the Federal Records Act, the Departmental Records Officer and bureau Records Officers are responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.