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: Enterprise Dashboard System (EDS)
Bureau/Office: Office of the Chief Information Officer
Date: October 4, 2016
Point of Contact:
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: Teri_Barnett@ios.doi.gov
Phone: 202-208-1605
Address: 1849 C Street NW, Mail Stop 5547 MIB, 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?

The Enterprise Dashboard System (EDS) is a component of the eMail Electronic Records and Document Management System (eERDMS), which is a program that provides the framework for storing, accessing, and managing Department of the Interior (DOI) records. EDS is used to report key statistical transactional data related to eERDMS. The dashboards within EDS are available on the DOI BisonConnect eERDMS site accessible by all DOI employees, contractors, and volunteers who have a DOI Active Directory account.

Currently, EDS displays eERDMS processing data for:

1. Audit Gaps Dashboard provides information related to gaps in journaled emails or other legacy archives.
2. Discovery and Collection Dashboard provides a status report on requests related to Freedom of Information Act, litigation, investigation case file, congressional or administration records, or other collections within the eERDMS component systems.
3. Journaling Statistics Dashboard contains statistical information related to inbound and outbound emails from BisonConnect, the Department's information management tool that contains a suite of Google applications and tools including email, calendar, instant messaging, document development, collaboration and production and cloud storage applications.
4. Program Tasks Dashboard provides a list of high-level programmatic tasks for each major component systems of the eERDMS, and other mission related operational groups such as communication and support.
5. Storage Statistics Dashboard provides information on the data stored by each bureau and office and the bureau and office projects.

EDS has the capability to develop additional dashboards depending on the business need and mission. This PIA will be revised as additional dashboards are developed and to address any privacy implications.

C. What is the legal authority?

The Department of the Interior, Establishment, 43 U.S.C. 1451; Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. 3501; the Clinger-Cohen Act of 1996, 40 U.S.C. 1401; 43 CFR Public Lands: Interior; OMB Circular A-130, Managing Information as a Strategic Resource; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service", April 27, 2011; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments", December 8, 2011; Presidential Memorandum, "Building a 21st Century Digital Government", May 23, 2012; OMB M-12-18, "Managing Government Records"; OMB M-13-13 "Open Data Policy - Managing Information as an Asset"; 36 CFR 1220: Federal Records, General; Presidential Memorandum, "Managing Government Records", November 28, 2011.

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?
The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

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

010-000000312, eMail Enterprise Records and Document Management System System Security Plan

☐ 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)*

☒No

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

☐ Yes: *Describe*
☒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
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☐ Financial Information
☐ Medical Information
☐ Disability Information
☐ Credit Card Number
☐ Law Enforcement
☐ Education Information
☐ 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

☐ Legal Status
☐ Place of Birth
☐ Emergency Contact
☐ Driver's License
☐ Mailing/Home Address
☐ Race/Ethnicity
☒Other: *Specify the PII collected.*

The Audit Gaps Dashboard within EDS contains the name and official email address of bureau or office points of contacts requesting an audit. The Program Tasks Dashboard contains the sponsor name and name of the individual assigned to complete a task within the eERDMS various component systems. The Discovery and Collection Dashboard contains names of the individuals requesting auditing information in support of litigation, FOIA, Congressional and Administrative Record, and Controlled Unclassified Information. This data is collected using Google Sheets and displayed on the Google Site where EDS is located with BisonConnect.

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: *Describe*

Information in the dashboard is derived from eERDMS component systems and entered by eERDMS management staff. For example, the Departmental Audit Request Form is a form completed to request records collections. The name of the requestor is noted on the Discover and Collection Dashboard. Another example is the Program Tasks Dashboard logs tasks by various tasked employees in support of eERDMS. The name of the responsible employee is noted on this dashboard along with the associated task.

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: *Describe*

PII collected for the Discover and Collection Dashboard and Program Tasks Dashboard are manually captured in a Google Sheet document and displayed in the dashboards located on the Google Site.

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

The intended use of the PII such as name and email address for the Discover and Collection Dashboard and Program Tasks Dashboard is to ensure various managers supporting the eERDMS program and the users they interact with during the course of normal business are aware of the status of these activities. PII collected in the Audit Gap Dashboard provides a bureau or office point of contact to assist with obtaining records which are not contained within eERDMS. The name of the requestors in the Discovery and Collection Dashboard are used to track individuals that submitted the collection request and whom to send the results. PII collected in the Program Tasks Dashboard is used to track the status of the tasks and determine who assigned the task and the individual accountable for the task.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

PII is shared with DOI employees, contractors, and volunteers who access the system through their DOI Active Directory account and is used to report key statistical transactional data related to eERDMS.

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

PII is shared with DOI employees, contractors, and volunteers who access the system through their DOI Active Directory account and is used to report key statistical transactional data related to eERDMS.

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

Information may be shared with other Federal agencies as and authorized and required to meet legal and reporting requirements.

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

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

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

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

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

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

Individuals have the opportunity to decline to provide information in support of the Discovery and Collection Dashboard and the Program Tasks Dashboard; however, employees, program offices, and sponsors will be unable to track the status of their tasks within eERDMS.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

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

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

☐ Privacy Notice: *Describe each applicable format.*

☐ 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.).

Data in the dashboard is not retrievable or searchable. EDS is read-only for DOI employees, contractors, and volunteers who access to the system through their DOI Active Directory account. eERDMS management staff will enter the data in the Google Sheet document for the respective dashboards.

I. Will reports be produced on individuals?

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

☒No

Section 3. Attributes of System Data

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

EDS reports key statistical transactional data derived from eERDMS, and is not collected from other sources.

B. How will data be checked for completeness?

It is the responsibility of the individual entering data into the Discovery and Collection Dashboard and Program Tasks Dashboard to check for the completeness of the data. Those individuals are responsible for ensuring the name of the individual is correct by verifying the information with the appropriate points of contact within the program office.

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

It is the responsibility of the individual entering data into the Discovery and Collection Dashboard and Program Tasks Dashboard to check for the currency of the data. Those individuals are responsible for ensuring the name of the individual is correct by verifying the information with the appropriate points of contact within the program office.

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

Data in EDS is maintained under DOI record schedule DAA-0048-2013-0001-0003 - 1.1C Administration Records of Specific Temporary Value. The retention period is cut off when the object or subject the records refer to is removed/discontinued (e.g., commission terminated, register/list superseded, temporary structures removed, etc.). See specific bureau/office instructions for individual cases. Records are destroyed when no longer needed.

Retention periods for potential records captured by eERDMS vary according to agency needs and specific subject matter, and are retained in accordance with applicable Departmental, bureau or office records retention schedules, as approved by the National Archives and Records Administration (NARA). Records retention periods are also subject to litigation holds, court orders, and preservation notices issued by the Office ofthe Solicitor. System administrator logs are covered by NARA's General Records Schedule 20(1)(c).

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

The raw data contained within the Journaling Statistics Dashboard and Storage Statistics Dashboard is continuously updated when new data is captured from eERDMS. Data contained within the Discovery and Collection Dashboard and Program Tasks Dashboard that have been completed are manually removed from the Google Sheet document. Google Sheet maintains a log of the revision history. DOI records are disposed of by shredding or pulping paper records, and degaussing or erasing electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

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.

The information within the EDS contains statistical data and non-sensitive PII. There is a low privacy risk associated with EDS because this information is work-related and is not sensitive, and the system reports statistical transactional data related to eERDMS.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒Yes: *Explanation*

The data in the EDS dashboards are relevant and necessary for tracking tasks and reporting statistical transactional data related to eERDMS to meet DOI business needs and missions.

☐ 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?
EDS does not derive new data about an individual.

F. Are the data or the processes being consolidated?

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

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

☒No, data or processes are not being consolidated.

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

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

DOI employees, contractors, and volunteers who have a DOI Active Directory account have access to the system and Google Sites, which allows the users to view the dashboards. Employees managing the Discovery and Collection Dashboard Dashboard and Program Tasks Dashboard and related Google Sheets have direct access to that specific data.

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

DOI employees, contractors, and volunteers who have a DOI Active Directory account have access to the system and Google Sites, which allows the users to view the dashboards. Employees managing the Discovery and Collection Dashboard Dashboard and Program Tasks Dashboard and related Google Sheets have direct access to that specific data.

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?*

☒No

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

☐ Yes. *Explanation*

☒No

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

☐ Yes. *Explanation*

☒No

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

The system does not have the capability to identify, locate, and monitor individuals therefore no information is collected as a function of monitoring individuals.

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

The system does not have the capability to identify, locate, and monitor individuals therefore controls are not used to prevent unauthorized monitoring.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

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

The key statistical data derived from eERDMS which is displayed on the EDS is secured through network 443 portal addressing. The connection between the Google Site and eERDMS is secured following NIST 800-53 controls.

(3) Administrative Controls. Indicate all that apply.

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

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Deputy, Information and Technology Management Division, Office of the Chief Information Officer, is the EDS Information System Owner and the official responsible for oversight and management of the EDS security and privacy controls. The EDS Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in EDS.

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 EDS Information System Owner is responsible for oversight and management of the EDS security and privacy controls, and is responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC and US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the Departmental Privacy Officer.