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: Electronic Drawing Repository and Automated Workflow Solution (eDRAWS)

Date: 06-08-2016

Bureau/Office: Reclamation/Information Resources Office Information Ma

Bureau/Office Contact Title: Reclamation Drawing Manager

Point of Contact Email: dwitbak@usbr.gov

First Name: Diane

M.I.:

Last Name: Witbak

Phone: (303) 445-3698

Address Line 1: Denver Federal Center, Bldg. 67, 12th Floor

Address Line 2: PO Box 25007

City: Denver

State/Territory: Colorado

Zip: 80225

Section 1. General System Information

A. Is a full PIA required?

Yes

Yes, information is collected from or maintained on

Federal personnel and/or Federal contractors

B. What is the purpose of the system?

The Electronic Drawing Repository and Automated Workflow Solution (eDRAWS) is a drawing management system used for the creation, revision, workflow, and management of engineering drawings critical to the mission of the Bureau of Reclamation and its business practices. The Meridian Enterprise software, eDRAWS, is integrated with the DOI Active Directory system. The eDRAWS software is BlueCielo's Meridian Enterprise ECM software, version 2016. The eDRAWS application does not maintain sensitive PII. It uses names and usernames to authenticate users within the DOI network, to assign and manage tasks, and facilitate drawing approval workflow within the application.

Managing engineering drawings as official records is a critical and integral part of Reclamation's daily business. Engineering drawings are vital representations of the infrastructure that facilitates delivering water and generating power to more than 31 million people. A successful drawing management system needs to provide the capability to capture relationships between drawings, share drawings between users and regions, allow for and manage version control; re-use prior designs in order to reduce the cost of future designs and drawings; keep track of nested relationships between the computer aided design (CAD) file of the drawing and other files; capture title block meta-data syncing; and support hybrid files which have been scanned and layered. The record aspects of an engineering drawing are complex and need to be captured and maintained so that the integrity of the drawing is not lost. Additionally, an electronic drawings management system must also manage its storage space efficiently in order to eliminate the need for redundant storage. eDRAWS enables Reclamation to efficiently manage and quickly retrieve drawing records as required for legal inquiries.

The Information Management Group (IMG) of the Information Resources Office (IRO) is the eDRAWS Program Office. The Manager of the IMG is the Business Owner of eDRAWS and the Reclamation Assistant Director of Information Resources (ADIR) is the Executive Owner.

C. What is the legal authority?

5 U.S.C. 301; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); and Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; and Federal Records Act (44 U.S.C. 3101).

D. Why is this PIA being completed or modified?

Existing Information System under Periodic Review

E. Is this information system registered in CSAM?

Yes

Enter the UII Code and the System Security Plan (SSP) Name

010-000001519, System Security Plan for Electronic Drawing Repository and Automated Workflow Solution

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

Subsystem Name	Purpose	Contains PII	Describe
None	None	No	

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

No

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

No

Section 2. Summary of System Data

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

- [x] Name
- [ ] Citizenship
- [ ] Gender
- [ ] Birth Date
- [ ] Group Affiliation
- [ ] Marital Status
- [ ] Biometrics
- [ ] Other Names Used
- [ ] Truncated SSN
- [ ] Legal Status
- [ ] Place of Birth
- [x] Other
- [ ] 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

Specify the PII collected.

eDRAWS contains engineering drawings and uses usernames from the Active Directory system to authenticate users within the DOI network and to assign and manage tasks. Username consists of first initial, last name, or, first and middle initial, last name. The eDRAWS system is integrated with Active Directory and the username that is populated in eDRAWS is retrieved from Active Directory. It is not entered by the user into the Meridian Enterprise application software. Scanned copies of engineering drawings may contain officials' signatures for review, approval and design.

B. What is the source for the PII collected? Indicate all that apply.

- [ ] Individual
- [ ] Federal agency
- [ ] Tribal agency
- [ ] Local agency
- [x] 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
- [x] Other
- [ ] Telephone Interview
- [x] Information Shared Between Systems

Describe

The user's name and username data in eDRAWS is extracted from integration with the DOI Enterprise Active Directory system, which authenticates users on the DOI network.

When a user launches the eDRAWS application the' user's name' and their 'username' are captured in system audit logs, which provide a chronological record of information system activities, including access and operations performed by a specific user, and documented with a date and time stamp. Additionally, the user's name and usernames are captured in the application 'To-Do' list within the software to facilitate the drawing approval workflow.

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

To authenticate users accessing eDRAWS within the DOI network, to assign and manage tasks, and facilitate drawing approval workflow for engineering drawings within the application.

User's names and 'usernames' are collected in the automated audit logs that provide a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant action from inception to final result. Additionally, the user's name and usernames are captured in the application 'To-Do' list within the application software to facilitate the drawing approval workflow. Names of individuals are associated with groups that determine access/permissions within the application.

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

- [x] Within the Bureau/Office

Describe the bureau or office and how the data will be used.

The BOR eDRAWS Systems Administrators (authorized employees only) review and analyze eDRAWS audit records for indications of inappropriate or unusual activity and report findings to designated BOR officials.

☐ Other Bureaus/Offices

☐ Other Federal Agencies

☐ Tribal, State or Local Agencies

☒ Contractor

Describe the contractor and how the data will be used.

The Contractor eDRAWS Systems Administrators (authorized employees only) review and analyze eDRAWS audit records for indications of inappropriate or unusual activity and report findings to designated BOR officials.

☐ Other Third Party Sources

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

Yes

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

eDRAWS users see a login banner and must acknowledge and consent to having their actions on the system and DOI network monitored. Below is the Reclamation Warning Banner:

"WARNING TO USERS OF THIS SYSTEM, THIS IS A NOTICE OF MONITORING OF THE DEPARTMENT OF THE INTERIOR (DOI) INFORMATION SYSTEMS.
This computer system, including all related equipment, networks, and network devices (including internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems may be monitored for all unlawful purposes; including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative or other adverse action. Unauthorized or illegal use may subject you to prosecution."

If individuals/contractors do not accept the login banner by clicking OK then logon access is not granted.

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

☐ Privacy Act Statement ☒ Privacy Notice ☒ Other ☐ None

Describe each applicable format.

A Privacy Notice is included in the eDRAWS User Account Request Form.

AUTHORITY: 5 U.S.C. 301; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501);
the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); and Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
PRINCIPLE PURPOSE: To provide a common authoritative directory service for the purpose of ensuring the security of DOI computer networks, resources and information, and protecting them from unauthorized access, tampering or destruction. To authenticate and verify that all persons accessing DOI computer networks, resources and information are properly authorized to access them.
ROUTINE USE: Use and disclosure of the information collected may occur in accordance with the following System of Record Notices: DOI-47. Information may be released to the Department if it has been determined that as a result of a suspected or confirmed compromise there is a risk of harm to economic or property interest, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information.
DISCLOSURE IS VOLUNTARY: If the requested information is not provided then access may not be granted to DOI computer networks, resources and information.

Users also receive notice of the uses of their information through the publication of this eDRAWS privacy impact assessment and the DOI-47 Logical Security Files system notice.

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

Audit data and logging of all actions occurs within the Meridian Enterprise software. The system will audit for the minimum requirements as defined by the DOI Security Control Standard for Audit and Accountability Controls. Reporting is set to include audit records that contain sufficient information, including: what type of event occurred; date and time of the event; where the event occurred (which eDRAWS hub server); the source of the event; the outcome of the event; and the identity of any user or subject associated with the event.

I. Will reports be produced on individuals?

Yes

What will be the use of these reports? Who will have access to them?

Within the eDRAWS application 'reports' can be generated to show what drawing files are on a particular user's To-Do list. These types of reports are accessible to any authorized eDRAWS user that is a member of specific application security roles containing the required permissions and privileges. These types of reports can be used to facilitate workload either by re-assigning items on a To-Do list or allocating additional resources.

Logging of all actions occurs within the Meridian Enterprise software. The system will audit for the minimum requirements as defined by the DOI Security Control Standard for Audit and Accountability Controls. Reporting is set to include audit records that contain sufficient information, including: what type of event occurred; date and time of the event; where the event occurred (which eDRAWS hub server); the source of the event; the outcome of the event; and the identity of any user or subject associated with the event.

Section 3. Attributes of System Data

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

The eDRAWS system does not collect data from sources outside of the DOI. The user can only access the eDRAWS system as a valid, authorized Active Directory user with current and accurate credentials, an active authorized PIV card, and a valid and authorized eDRAWS user account. eDRAWS is an IT system internal to the Bureau of Reclamation only.

B. How will data be checked for completeness?

The DOI Enterprise Active Directory system will authenticate the user's "username" and credentials when the user logs into the Reclamation network, and these usernames and credentials are kept current by the Active Directory system. If the user does not have a valid, authorized eDRAWS account (membership in an application security role/group) they cannot perform any activities within the application.

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

eDRAWS user's names and 'usernames' are kept current by updates to the DOI Enterprise Active Directory system, which is managed by the AD Administrators, and the eDRAWS User Account form.

Electronic eDRAWS User Account forms are kept on the internal eDRAWS SharePoint site, which is maintained by the Reclamation Enterprise Service Center (RESC) Helpdesk and the IMG eDRAWS Information System Security Officer (ISSO).

Standard Operating Procedures (SOP) for user account management is maintained by the eDRAWS ISSO and provided to the RESC. The SOP is updated as changes occur to the account management process.

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

The eDRAWS system and the records it contains is classified as a Permanent system according to PRJ-27.00 'Drawings and Design Data.' Specifically, "Official File Copy - PERMANENT – Retain current revision in Reclamation for 5 years. Transfer to FRC or National Archives in Denver at conclusion of activity or as volume warrants."

Records relating to persons covered by Active Directory are retained in accordance with a separate records schedule,

identified as item 7561 of the Office of the Secretary Records Disposition Schedule. Disposition is temporary, cut off upon expiry of the ID card. Destroy after 3 years after cut-off. (DRS 1.1A DAA-0048-2013-0001-0001).

Audit logs in eDRAWS inherit the retention of the drawing record that it is associated with; therefore, audit logs are Permanent.

Drawing records that are not official file copies are 'marked for deletion' by the eDRAWS user, reviewed and then marked 'approved for deletion' by the Super Drawing Manager (specific individuals for each region with 'Delete' privileges), and then a Purge is run on the eDRAWS server which clears out all of the drawing records that were marked and approved for deletion.

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

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for 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.

eDRAWS does not collect and maintain sensitive PII so there is minimal risks to the privacy of individuals. eDRAWS is necessary to perform workflow functions for engineering drawings and to comply with related Federal laws and regulations. To prevent misuse (e.g., unauthorized browsing) eDRAWS users submit a User Account Request form to the RESC and eDRAWS Admins and Information System Security Officer (ISSO) to clearly establish and document user security roles and responsibilities. The user data in eDRAWS is extracted from the integration with the DOI Enterprise Active Directory system to authenticate users and support application workflow processes required for the lifecycle of engineering drawings.

The eDRAWS system has undergone a formal Assessment and Authorization and has been granted an authority to operate (ATO) in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology standards. eDRAWS is rated as FISMA moderate based upon the type of data and requires strict security controls to protect the confidentiality, integrity, and availability of the data contained in the system. eDRAWS application roles define specific access and permissions and individuals are granted access and permissions based on the role membership they request. eDRAWS users must have a valid and authorized DOI Enterprise Active Directory account and their request for access to eDRAWS must be authorized and approved by the individual's Supervisor and the Drawing Approval Authority for their office.

Separated employees are removed from Active Directory, which effectively removes individual access to the DOI network and to eDRAWS. Once a user is removed from the Active Directory groups for eDRAWS the user's name and 'username' no longer appear in the drop down list for the To-Do list. The synchronization between Active Directory and eDRAWS is a one way add/update, so no deletes of the username in the local user database occur.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. Audit trails of activity are maintained to reconstruct security relevant events. The audit trail will include the identity of each user accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The eDRAWS system follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Reclamation employees and contractors are required to complete security and privacy awareness training and sign DOI Rules of Behavior.

All user's names and 'usernames' captured by eDRAWS in the audit logs and To-Do lists are protected by giving access only to valid, authorized personnel. This information is not shared outside of Reclamation as eDRAWS is for internal use only. Backups of the data can only be accessed by valid, authorized users within Reclamation. When eDRAWS reaches end of life the equipment and/or media that contains user's names, 'usernames,' and audit logs will be retained per the retention schedule for Information Technology systems and then destroyed.

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

eDRAWS is a drawing management system used for the creation, revision, workflow, and management of engineering drawings critical to the mission of the Bureau of Reclamation and its business practices.

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

No

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

No

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

No

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

eDRAWS does not derive new data.

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.

Audit logs are consolidated for correlation, alerting, notification and reporting. Audit logs are primarily utilized for forensic and investigative purposes and used by System Administrators. Audit logs produced are configured to include type of event, the host that originated the log message, the date and time the event occurred, the application or command generating the event, the outcome of the event. Audit information is restricted to authorized-personnel only and designated in AD security groups. These processes and procedures are outlined in the internal eDRAWS System Security Plan.

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

☒ Users ☒ Developers ☒ System Administrator

☒ Contractors ☒ Other

Describe

All eDRAWS authorized users can view the system 'To-Do' lists, where user's names and 'usernames' are captured, showing the files which are currently assigned to a specific user. Users belonging to the 'Editor' or above application security group can re-assign the files to another user as needed but they cannot delete a user nor the drawing record files they are working on. Contractors fill both the end-user role and the system administration roles. Developers for the software vendor can access an eDRAWS server to provide support and they can view user's names and usernames, but cannot disable or delete a user or their access. The eDRAWS Administrator/Configurator and Information System Security Officer (ISSO) have access to the audit logs within eDRAWS.

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

User access to data is determined by the application role they select which is best designated for the work they need to perform within the eDRAWS system. Selection of the role is made via the eDRAWS User Account Request form and is approved by the individual's Supervisor and the designated Drawing Approval Authority for that eDRAWS hub/region. eDRAWS users are able to view other users' names and usernames during the workflow processes inherent in the system.

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?

The eDRAWS IDIQ Contract and Reclamation Task Order contain the FAR Privacy Act clauses, and will be modified to include additional DOI contract provisions.

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

No

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

Yes

Explanation

eDRAWS generates audit logs containing information that establishes the following: what type of event occurred; date and time of the event; where the event occurred (which eDRAWS hub server, which is associated with a regional or area office); the source of the event; the outcome of the event; and the identity of any user or subject associated with the event. User names can be associated with any of the following events in the audit logs: account management events, object access, privilege functions, process tracking, system events, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Audit logs and audit monitoring tools are restricted to authorized personnel only.

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

eDRAWS generates audit logs containing information that establishes the following: what type of event occurred; date and time of the event; where the event occurred (which eDRAWS hub server, which is associated with a regional or area office); the source of the event; the outcome of the event; and the identity of any user or subject associated with the event. The eDRAWS system does not collect any information about user logons of any type.

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

BOR fully complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any eDRAWS equipment. The use of DOI and BOR IT systems, including eDRAWS, is conducted in accordance with the appropriate DOI and BOR use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Access to eDRAWS audit logs and audit tools are restricted to authorized personnel only via access control lists and authorized access to the eDRAWS dashboard. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. The eDRAWS system follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. All Reclamation employees and contractors are required to complete security and privacy awareness training and sign DOI Rules of Behavior.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

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

Describe

Only valid, authorized individuals with membership in the appropriate eDRAWS application roles and security groups have access to eDRAWS.

(3) Administrative Controls. Indicate all that apply.

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

Describe

eDRAWS access is managed via an authorized, valid account in the Active Directory domain. Access with the AD Domain is managed by the DOI Enterprise Services Network (ESN).
Regular monitoring of User's security practices is performed through the monitoring activities as designated by the Reclamation Mission Support System. Audit features provide notifications of unauthorized use and system activities.

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 eDRAWS Information System Owner is responsible for oversight and management of the eDRAWS security and privacy controls and the protection of information stored in the eDRAWS system. The Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented in compliance with Federal laws and policies for the data managed and stored in eDRAWS.

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