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: Denver Office Reclamation Services and Applications Mission Support - Research and Development Information Management System (RADIMS)
Bureau/Office: Bureau of Reclamation/Denver Office
Date: 4/10/2018
Point of Contact:
Name: Regina Magno
Title: Associate Privacy Officer
Email: privacy@usbr.gov
Phone: 303-445-3326
Address: PO Box 25007, Denver, CO 80225

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?

RSAMS-RADIMS
The Denver Office Reclamation Services and Applications Mission Support (RSAMS) - Research and Development Information Management System (RADIMS) is an internal

application intended to serve Reclamation's Research and Development Office (R&D) to support management efficiencies of its Science and Technology Program (S&T).

Reclamation's Research and Development Office, Science and Technology Program
R&D applies science and technology to advance the bureau's mission to manage, develop, and protect water and water-related resources in an environmentally and economically sound manner in the interest of the American public. S&T's annual Research Solicitation cycle is a competitive, internal research program that awards the following Fiscal Year's (FY) budget dollars to Reclamation employees who have the time and permission to lead applied research projects as the Principal Investigator (PI). The PI may conduct the research, or may lead a team of internal (Reclamation) researchers, external (non-Reclamation) researchers, stakeholders and advisors. S&T goals are to:

1. Develop cost-effective solutions for the technical and scientific problems affecting accomplishment of Reclamation's mission, while leveraging funds with other research entities to advance research in a collaborative manner.
2. Build and strengthen scientific and engineering capacity for Reclamation in order to advance the most relevant research and demonstration projects for Reclamation.
3. Communicate those solutions to Reclamation offices, other water and power management officials, and the general public in order to build partnerships with other water and power management agencies and stakeholders.

Funding under the S&T Program is allocated based on relevance and technical scoring criteria identified as follows:

- Research Area
- Research Category
- Need, Benefit, and Urgency
- Communication Plan
- Application Potential
- Research Question
- Research Strategy
- Key Person Qualifications
- Budget

RADIMS Scope and Purpose
Developed by Reclamation's Information Technology Services – Application Services Group, RADIMS is the replacement solution for R&D's Proposal and Performance Contract Management System (PropC). RADIMS automates the business practices and workflow processes for the S&T program and is essential to the operation of the S&T program's annual Research Solicitation cycle, which includes: research proposal submission, review, selection, project management, and program management processes. Once fully deployed, RADIMS will support all facets of the S&T program's management phases.

RADIMS allows for the electronic submission of research Proposals by Reclamation employees, referenced previously as PIs, serving in the Researcher role. Proposals include the following: summary, research strategy (which identifies Key Persons who may be Reclamation employees or individuals outside of Reclamation), partnership (which identifies Partners who may be Reclamation employees or individuals outside of Reclamation), proposed budget, need, quality control, risk management, communication plan, implementation plan, and approvals.

After a proposal is submitted, RADIMS creates a PDF of the proposal and emails it to the reviewers. The proposal is subjected to two distinct review teams. The first is by Independent Technical Reviewers (subject matter experts outside of Reclamation) who evaluate the technical merits of the proposal. The second is by Program Panel Reviewers (Reclamation employees) comprised of R&D's S&T Research Coordinators and Regional S&T Research Coordinators.

Once funding decisions are made, RADIMS sends an e-mail to the Researcher notifying them of funding data. This portion of the system is not considered a financial management application but simply automates the R&D funding processes. In future development phases, RADIMS will integrate with Reclamation's instance of the Financial and Business Management System (FBMS), the Department-wide integrated finance and administrative system that supports standard business management practices, to accept FBMS updates to funded projects via automated data push technology. RADIMS will not push data back to FBMS. The data provided by FBMS Fund Detail to RADIMS does not include PII, and will only include the following budget related data fields for execution reporting:

- Funding Agreement (FA) Budget Activity
- Fund
- Funded Program
- Funds Center
- Recoveries
- Carryover of Past Year (PY) Unobligated Balances
- Total Realized Budgetary Authority
- Total Obligations
- Calendar Year (CY) Obligations
- Total Expenditures
- Disbursements
- Gross Outlays
- Cumulative Unexpended
- Committed But Not Obligated
- Undelivered Orders (UDO)
- UDO including Recoveries and PY Upward Obligations
- Consumable Budget
- Total Committed + Total Obligated
- Total Currently Available for Obligation
- Uncommitted Budget Available
- Concatenated Fund Work Breakdown Structure (WBS)

RADIMS also supports project management by automating change order requests as well as closeout requirements. RADIMS accepts uploads of PDFs submitted by the

Researcher related to research project products, including Section 508 compliant Final Reports and Research Bulletins, and pushes the product(s) to the respective S&T public-facing Project webpage at https://www.usbr.gov/research/projects/index.html to disseminate research results.

C. What is the legal authority?

RADIMS is consistent with all applicable laws, regulations and policies, which include: The Reclamation Act of 1902, (Pub. L. 57-161, as amended); Federal Technology Transfer Act of 1986 (Pub. L. 99-502; 15 USC 3710A); Omnibus Public Land Management Act of 2009 (Pub. L. 111-11); America COMPETES Reauthorization Act of 2010 (Pub. L. 111-358)

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*

UII Code: 010-000000299-00-10-01-03-01-00
System Security Plan Name: Denver Office Reclamation Services and Applications Mission Support - Research and Development Information Management System

☐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	N/A	N/A	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: This system is not a Privacy Act system of records.

Note: This system is not a Privacy Act system and does not maintain records on individuals, however, employee names, usernames and contact information are covered under the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS)" system of records notice.

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
☒Other: *Specify the PII collected.*

For Reclamation employees, the PII collected is associated with the Reclamation Active Directory of employees, which includes: Last Name, Middle Name, First Name, Work Email, Work Organization, Work Department, Bureau, and Region.

For Key Persons/Partners not employed with Reclamation, the Key Person who is a Reclamation employee will add the non-Reclamation individuals' PII in RADIMS, which includes: Last Name, Middle Name, First Name, Work Email, Organization Name, and Organization Type.

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*

The RADIMS user attains PII from the individual (Key Person/ Partner if applicable) and inputs the PII for their respective research proposal/project into RADIMS. The RADIMS database is also linked to Reclamation's Active Directory, which provides PII for Reclamation employees to authenticate and control access to the system.

C. How will the information be collected? Indicate all that apply.

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

For the S&T Research Solicitation cycle, the RADIMS user collects the information. The Reclamation Researcher determines the method of collection for the Key Person/ Partner.

The RADIMS user logs onto RADIMS via an internal website using their Reclamation Active Directory credentials, similar to other Reclamation enterprise systems, to generate the information shared between RADIMS and the Active Directory systems.

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

The intended use of the PII collected is to help facilitate R&D communication during the annual S&T Research Solicitation cycle and throughout the project management cycle.

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.*

For the Research Solicitation cycles, the PII is shared within the Bureau of Reclamation's Research and Development Office as well as all Reclamation Directorates during Red Flag Review (the process where other directorates within Reclamation have an

opportunity to review the projects being recommended for funding, which helps avoid duplication of effort, policy conflicts, or other problems that were not caught earlier in the process) for Projects Selected for Funding. The PII is used to help facilitate R&D communication with R&D Staff from proposal, and, if funded, throughout the project management cycle.

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

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

☐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.*

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

For the Research Solicitation cycle, R&D communicates with Independent Technical Reviewers (subject matter experts outside of Reclamation) who evaluate the technical merits of the proposal, including determining whether team members are qualified.

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.*

Key Persons/Partners who are not Reclamation employees voluntarily provide their name and contact information to the Reclamation Researcher in order to participate in projects. Participation is not required and individuals may choose not to provide their information or participate in a project.

Reclamation employee information is voluntarily provided when requesting access to the DOI network and information systems, and normally occurs during the onboarding process and is required to enforce access controls across the DOI network. If users decline to provide the requested information they will not be given access to the DOI network or RADIMS.

☐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.*

Notice is provided through publication of this PIA. Employees may also view the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice for more information about how user credentials are managed.

☒Other: *Describe each applicable format.*

The following banner alerts users at the system's login screen:

***WARNING TO USERS OF THIS SYSTEM ***

This is a United States Government computer system, maintained by the Department of the Interior, to provide Official Unclassified U.S. Government information only. Use of this system by any authorized or unauthorized user constitutes consent to monitoring, retrieval, and disclosure by authorized personnel. USERS HAVE NO REASONABLE EXPECTATION OF PRIVACY IN THE USE OF THIS SYSTEM. Unauthorized use may subject violators to criminal, civil and/or disciplinary action.

The following banner is posted on the RADIMS site:

United States Bureau of Reclamation
Denver Office Reclamation Services and Applications Mission Support - Research and Development Office Information Management System (RADIMS)

This is a United States Government computer system, maintained by the Department of the Interior, to provide Official Unclassified U.S. Government information only. Use of this system by any authorized or unauthorized user may be monitored, recorded, retrieved, disclosure and subject to audit by authorized personnel. USERS HAVE NO REASONABLE EXPECTATION OF PRIVACY IN THE USE OF THIS SYSTEM. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties. The use of the information system indicates consent to monitoring and recording.

By clicking the link below the user acknowledge the usage conditions.

Continue to the RADIMS application

☐None

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

Information in this system is used to monitor and track proposals submitted by employees. User information is only used to manage access controls, authenticate authorized users, and track user activity as a security function. Proposals/Projects are only tracked by the respective ID assigned to proposals/projects that are randomly generated. There is no tracking in RADIMS by PII. PII included from members of the public, i.e., Key Persons and/or Partners identified in RADIMS from the Principal Investigator submitting their Proposal, is limited to name and official contact information. This information is collected and shared with the two research proposal review teams: 1) Independent Technical Reviewers (subject matter experts outside of Reclamation) who evaluate the technical merits of the proposal; and 2) the Program Panel Reviewers (Reclamation employees) comprised of R&D's S&T Research Coordinators and Regional S&T Research Coordinators.

I. Will reports be produced on individuals?

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

Reports are not produced on individuals but on the actions of users. If actions show unusual or malicious, etc. behavior the logs can correlate the actions taken in the system with a username. Reports can be generated to include any of the following events: successful and unsuccessful account logon events, account management events, object access, and privilege functions. Only systems administrators and the information system owner will have access to the activity reports.

☐No

Section 3. Attributes of System Data

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

The RADIMS application interface implements data input validation at entry. The user validates their information within the system. System Administrators validate data throughout a project's lifetime.

For the S&T Research Solicitation cycle, the Researcher collects the data directly from Key Persons/Partners who are not affiliated with Reclamation. The method of collection and verifying for accuracy is up to the discretion of the Researcher. The information collected for Key Persons includes: Last Name, Middle Name, First Name, Email, Organization Name. The information collected for partners includes: Last Name, Middle Name, First Name, Email, Organization Name, Organization Type (either Federal or non-Federal).

B. How will data be checked for completeness?

The Researcher collects the data directly from Key Persons/Partners who are not affiliated with Reclamation so their data is presumed to be complete. The DOI Enterprise Active Directory system will authenticate the user's credentials when the user logs into the RADIMS system.

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

The Researcher collects the data directly from Key Persons/Partners so the data is presumed to be current at the time it is provided. User information is kept current by updates to the DOI Enterprise Active Directory system.

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

Records in this system are covered under the Reclamation records retention schedule RES-1.10 "General Research Program Management" under the National Archives and Records Administration (NARA) approval authority N1-115-94-4, which is being incorporated into Departmental Records Schedule (DRS) 2.4.1.05 "Mission - Provide a Scientific Foundation for Decision Making - General Research Program Management", currently pending approval by NARA. Until DRS-2 is approved, the RADIMS records are maintained for 15 years. Once DRS-2 is approved RADIMS records retention will be Temporary and will be cut off at the end of each calendar year. Transfer records to the Federal Records Center (FRC) at 10 years or earlier if volume warrants. Records are destroyed 15 years after cutoff.

Records on user activity are retained in accordance with DRS – Administrative schedule 1.4 A.1 – [0013] Short Term IT Records – System Maintenance and Use Records (DAA-0048-2013-0001-0013). The disposition is Temporary. Cut off when superseded or obsolete. See records manual for specific criteria that may determine when a record is obsolete or superseded. Destroy no later than 3 years after cut-off. For user activity

records, once user accounts are terminated in the system the records are removed in accordance with the DRS records retention schedule.

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.

The RADIMS system does not collect or maintain sensitive PII so there is minimal risk to the privacy of individuals. RADIMS manages research solicitations and only Reclamation employees and Key Person/Partner names, organization and official contact information, voluntarily provided, are used to track and manage proposals/projects. All information is maintained within the system control of the agency. Data transmission is encrypted with Transport Layer Security (TLS) controls. Continuous monitoring scripts automatically capture user audit logs which contain user login information, such as successful log-ins, failed log-ins, and account lockouts for the past 30 days. The user audit logs contain employee names, usernames, and date and time of attempted access.

The RADIMS system has completed a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology standards. RADIMS is rated as FISMA low based upon the type of data and requires security controls to protect the confidentiality, integrity, and availability of the data in the system. The RADIMS system roles define specific access and permissions and individuals are granted access and permissions based on the role membership they request.

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 is reported to the project manager who will report it to local and/or regional IT security. The RADIMS 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. RADIMS may only be accessed from within the DOI network. Reclamation employees and contractors are required to complete security and privacy awareness training and sign the DOI Rules of Behavior.

All user information is captured in the audit logs and the system is protected by giving access only to valid, authorized personnel. This information is not shared outside of Reclamation as the system is for internal use only. Backups of the data can only be accessed by valid, authorized users within Reclamation. When the system reaches end of life the equipment and/or media that contains user information and audit logs will be retained in accordance with the records retention schedule for Information Technology systems.

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*

R&D receives an estimated 150 project proposals from an estimated 100 unique submitters within Reclamation. The use of the data is both relevant and necessary to the purpose for which the system is being designed because RADIMS automates the business practices and workflow processes for S&T and is essential to the operation of S&T's annual Research Solicitation cycle, which includes: research proposal submission, review, selection, project management, and program management processes. This meets Federal regulation standards as authorized by Federal legislation, regulations, and policy to enable Federal agencies to make their research and development facilities and expertise available to the public.

☐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?

RADIMS 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.*

☐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*

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

Only Reclamation employees may access the system using their Reclamation Active Directory credentials, similar to other Reclamation enterprise systems. User roles are managed by System Administrators, including access permissions to different portions of the system. The Researcher role will only have access to the data they input and cannot access other users' data. The Budget Analyst role will only have access to budget data.

The S&T Staff role may only access project management review capabilities within the system. The System Administrator role will have access to all system information. System Administrators will monitor input processes.

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 developer used a standard Reclamation contract that included FAR Privacy Act Clauses and additional security and privacy provisions to protect DOI information systems and data.

☐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*

The system contains audit features that monitor users within the system for security purposes. The session logs capture user name, log in, log out, time stamp and any time the user is timed out. Another record account will capture any time a user makes a change to a table.

☐No

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

The system audit logs capture user name, log in, log out, timed out, time stamp, IP address and unsuccessful login attempts. These logs are captured and recorded in the Session Logs. The Record account will capture any time a user makes a change to a table.

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

Reclamation 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 are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration. The use of DOI and Reclamation IT systems is conducted in accordance with the appropriate DOI and Reclamation use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events, and will include the identity of users 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.

Only authorized users with system administrator privileges have access to monitor user's activities in the system. The RADIMS follows the NIST 800-53 controls and DOI security and privacy control standards for user access based on least privilege, ensuring that only authorized individuals are authorized to have access to system data.

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*

(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 Chief, Research and Development Office serves as the RADIMS Information System Owner and the official responsible for oversight and management of the security and privacy controls for the system. The Information System Owner and Information System Security Officer, in collaboration with the BOR Associate Privacy Officer, are responsible for ensuring adequate safeguards are implemented in compliance with Federal laws and policies for the data managed and stored in RADIMS.

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 RADIMS Information System Owner is responsible for oversight and management of the RADIMS security and privacy controls, and for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner is also responsible for reporting any loss, compromise, or unauthorized access to the system or data is reported to the DOI Computer Incident Response Center within one hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any potential compromise in consultation with the BOR Associate Privacy Officer.