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: NR STORET
Bureau/Office: National Park Service (NPS), Natural Resource Stewardship and Sciences (NRSS) Directorate
Date: October 7, 2020
Point of Contact:
Name: Felix Uribe
Title: NPS Associate Privacy Officer
Email: nps_privacy@nps.gov
Phone: 202-354-6925
Address: 12201 Sunrise Valley Drive, Reston VA 20192

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?

NR STORET encompasses two Commercial Off the Shelf (COTS) repositories of physical, chemical, biological, and other ambient water monitoring data collected in and around national park units by park staff, contractors, and volunteers. The repositories include:

(1) EarthSoft's Environmental Quality Information System (EQuIS) software and database for discrete (i.e. less than daily) lab samples, field measurements, and observations, and

(2) Aquatic Informatics' Aquarius time series software and database for continuous time-series (e.g. every 15 minute) water data.

The purpose of NR STORET is to centralize and archive water resource data for use in determining the status and trend of park water resources and to provide the data in human and machine-readable formats to the states (for Clean Water Act purposes) and the public. Only discrete lab samples, field measurements, and observations from EQuIS are transmitted in an XML file format to the National Water Quality Monitoring Council's Water Quality Portal (WQP) (https://www.waterqualitydata.us/) for public dissemination. The WQP is a cooperative service sponsored by the United States Geological Survey (USGS), the Environmental Protection Agency (EPA), and the National Water Quality Monitoring Council (NWQMC). It serves data collected by over 400 state, federal, tribal, and local agencies.

Continuous data from Aquarius Time-Series are disseminated via the NPS' AQWebPortal (Aquarius WebPortal: https://irma.nps.gov/aqwebportal/) which is part of the NPS' Integrated Resource Management Applications (IRMA) Portal.

No PII or sensitive data are transmitted to the Water Quality Portal or Aquarius WebPortal. Only DOI Personal Identity Verification (PIV) credentialed users (NPS employees, cooperators, and contractors) have access to the NR STORET subsystems. Cooperators are personnel working under a cooperative agreement with a university in the Cooperative Ecosystem Studies Units National Network. Cooperators and contractors work in NR STORET under the supervision of NPS staff.

Both the EQuIS and Aquarius subsystems are hosted on-premises on Windows Server infrastructure in the NPS Data Center managed by NPS employees and contractors and inherit privacy and security controls through the Data Center, the Department of the Interior's Enterprise Service Network (ESN), and National Park Service's General Support System network.

C. What is the legal authority?

- National Park Service Organic Act (54 U.S.C. 100101(a) et seq.)
- National Park Service General Authorities Act of 1970 (54 U.S.C. 100101(b) et seq.)
- National Parks Omnibus Management Act of 1998 (54 U.S.C. 100701 et seq.)
- Open, Public, Electronic, and Necessary Government Data Act (i.e. OPEN Government Data Act) which is Section 201 of the Foundations for Evidence-Based Policymaking Act of 2018 (P.L. 115-435)
- Clean Water Act (33 U.S.C. 1251-1387)

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*
NPS-NR STORET/WQX Water Quality Database System Security and Privacy Plan (010-000000573)

☐ 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.*
EQuIS	Manage discrete water quality (i.e. less than daily) lab samples and field measurements and observations.	Yes	Stores UserID and name of DOI users of the system. Optionally stores first and last names of the sample collector and data recorder. Sample location information (latitude and longitude coordinates) are recorded with the sample collection and are incidentally tied to the sample collector. Optionally stores the name of the laboratory (business name, address, first name, last name, phone number) that analyzed the samples.
Aquarius	Manage continuous (e.g. every 15 minute) water measurements	Yes	Stores UserID and name of DOI users of the system.

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

DOI Active Directory credentials are covered under:
DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) (March 12, 2007, 72 FR 11040)

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

☐ Yes: *Describe*
☒ No

NR STORET does not collect data from the public.

Section 2. Summary of System Data

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

☒ Name
☒ Other: *Specify the PII collected.*

Both EQuIS and Aquarius require users to authenticate using their DOI PIV credentials in order to access the software. NR STORET uses the UserID to enable authentication with PIV credentials and for audit logging purposes. An individual's first name and last name are associated with a UserID.

EQuIS allows optional entry of: (1) the first and last names of the person(s), potentially including volunteers, who collected the sample and/or recorded the data and (2) the contact information (business name, business address, first name, last name, and business phone number) for the laboratory that analyzed the sample.

The location (latitude and longitude) coordinates where the sampler collected the sample is recorded during sample collection and incidentally associated with the sample collector's information.

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:

The source of PII are DOI PIV credentialed users who access NR STORET (the NPS instances of EQuIS and Aquarius combined) to enter water-related data they have collected in or near their park or network. These DOI PIV credentialed users may, optionally, include the first and last names of the sample collector and/or data recorder, and the name of the lab that analyzed the sample. Only non-PII data is sent by XML transfer to the National Water Quality Monitoring Council's Water Quality Portal.

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:

Data is imported into NR STORET via structured electronic data deliverable (EDD) files. EDDs are accepted through electronic web forms over encrypted communication channels that comply with Federal standards. DOI PIV credentialed users enter the data from their field data collection forms, tablets, lab sample reports, and/or data sondes with electronic sensors, reformat the data into the appropriate EDD format, and, optionally, add their names as the sample collector and/or data recorder and the name of the lab that analyzed the sample.

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

The DOI PIV credentials are used for authentication to NR STORET. The optional PII (sample collector, data recorder, and lab name) is used for quality assurance/quality control. It provides information should questions arise about the data or the procedures used to collect or process the data. For example, if data analysis should reveal an unnatural or unexplained trend in the data, we might want to notify the collector/provider to inquire whether the trend is the result of extraneous environmental conditions, changes in analytical equipment, transcription errors, or some other issue before using the data as the basis to support resource management action.

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

☒ Within the Bureau/Office:

Only DOI PIV credentialed users have access to NR STORET. The PII (userid and optional sample collector, data recorder, and lab name) are not shared unless questions arise about the water data or the procedures used to collect or process it. If one of those situations arises, the PII could be used by NPS staff only to contact the data collector, recorder, or lab to inquire. Personnel authorized to access the system (DOI PIV

credentialed users) must complete all Security, Privacy, and Records Management training and sign the Rules of Behavior.

☐ 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.* No PII is shared with the National Water Quality Monitoring Council or any other Federal agency.

☐ 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.*

NPS contractors are involved with the installation and configuration of the software, application and database support, and management of the servers and other network infrastructure. Contractor and cooperator staff are required to undergo background checks as defined by NPS policy and procedures. Contractor and cooperator staff access will be restricted to data on a need to know basis. Privileged accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in the System Security Plan and Privacy Plan. This maintenance is critical to protecting the system and the PII contained within the system.

☐ 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:

The only PII that is required to use NR STORET is the user's DOI PIV credentials. For DOI credentialed users, information is collected from the individual during onboarding or generated as DOI records (e.g. email address, UPN, username) during operational activities. To establish an account for a DOI user, an authorized NPS manager emails (encrypted) a user account request to the NR STORET system administrator. The NR STORET system administrator creates the user account with the information provided, and the NR STORET system administrator queries the Active Directory Federated Services to validate and complete the account creation.

The sample collector, data recorder, and lab point of contact may decline to provide PII information simply by omitting the information from the water sample data provided.

Consent is assumed when PII information is provided by the sample collector, data recorder, or lab point of contact.

☐ 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 and the applicable published SORN. For NR STORET the NPS Privacy Policy is included on every web page as a section of the footer and directs the user to: https://www.nps.gov/aboutus/privacy.htm.

☒ Other: *Describe each applicable format.*

The only users of NR STORET are DOI PIV credentialed users who consent to using their active directory credentials when authenticating to EQuIS and Aquarius. At log on to the NPS network, the user must acknowledge the privacy notice applied to the NPS network.

☐ 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 are retrieved from EQuIS and Aquarius by location, parameter/characteristic/analyte, and date range in order to examine water-related status and trends and determine whether the water meets its state-designated beneficial uses (i.e. whether it is impaired under the Clean Water Act). Other than server user logs and audit logs, there is no data to retrieve by user.

I. Will reports be produced on individuals?

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

☐ No

Both EQuIS and Aquarius subsystems maintain internal audit logs that track the date/time of system access as well as data edits and deletions of DOI PIV credentialed users. No reports are generated, nor do they even exist. The audit logs and EQuIS' optional sample collector, data recorder, and lab name fields are only accessed by the system administrator for quality control purposes if a user reports that something is 'wrong' with the data.

Section 3. Attributes of System Data

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

Only DOI PIV credentialed users can access NR STORET and enter water-related data. DOI PIV credentialed users can also enter water-related data into NR STORET that they receive from universities, watershed management organizations, and other credible data collectors. Those organizations must collect their data under authorized NPS research permits and consent to having the results uploaded to NR STORET. Regardless of the data source, the potential PII data is still the same optional fields: EQuIS' sample collector, data recorder, and lab name. It is the responsibility of the DOI PIV credentialed user that enters water-related data into NR STORET to acquire approval from the data provider and appropriately quality assure and quality control the data. Water data can have a robust set of quality control measures that can be implemented to ensure credible data are collected. Additionally, double entry of data or 100% verification is common. Data providers can set attributes in EQuIS and Aquarius to indicate whether the water data are approved and/or certified. Only approved/certified data are disseminated to the public.

B. How will data be checked for completeness?

The EQuIS and Aquarius subsystems schemas both have required fields for documenting the results of environmental sampling, measurements, and observations. Data cannot be entered or saved in the database if the required fields are not complete. No PII is required, hence there is no need for a PII completeness check. In addition to system design, NR STORET relies on DOI PIV credentialed users to ensure data are complete.

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

Water data are typically collected to assess both status and trend. Consequently, both current and legacy data are useful and needed in the system. Regarding PII, its entry is optional and only part of the EQuIS system. Updating any optionally entered PII (sample

collector, data recorder, and lab name) is the responsibility of the DOI PIV credentialed data submitter.

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

Water Resource records in NR STORET are retained in accordance with the National Park Service Records Schedule, Resource Management and Lands (Item 1), which has been approved by the National Archives and Records Administration (Job No. N1-079-08-1). The disposition of Cultural and Natural Resource Management Program and Planning records is permanent. Periodic transfer of special media and electronic records along with any finding aids or descriptive information (including linkage to the original file) and related documentation by calendar year are transmitted to the National Archives and Records Administration (NARA) when 3 years old. Final transfer of all permanent records to NARA occurs 15 years after closure. Digital records will be transferred according to standards applicable at the time.

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

Workflows are in place to manage the disposition of permanent records in conformance with requisite retention schedules. Periodic transfer is accomplished through delivery of permanent special media and electronic records along with any finding aids or descriptive information (including linkage to the original file) and related documentation by calendar year to the National Archives and Records Administration (NARA) when 3 years old. Digital records, and their inherent machine-readable formats, will be transferred according to standards applicable at the time.

Final transfer of all permanent NR STORET records to NARA 15 years after closure is facilitated through direct exchange of machine-readable data sets with NARA. Transfer from NR STORET to NARA is facilitated by inherent retention logic which regulates release of information. Only users with AD credentials are able to contribute content to NR STORET systems, and only NPS personnel with AD credential can access the ARCIS so PII is protected throughout this process and the record's information lifecycle.

The approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with National Archives and Records Administration 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.

NR STORET is classified as a low-risk system. The Privacy risks associated with how information is handled in NR STORET during the information lifecycle are very low. All information acquisition and collection are done through electronic web forms over encrypted communication channels that comply with the required federal standards. Data are stored within an encrypted database to minimize risk of data breaches while in transit and while stored. Information access and retrieval is done through electronic web forms over encrypted channels following defined application security roles and permissions to ensure proper distribution and disclosure of information guided by the principle of least privilege to minimize the risk of improper information disclosure. The protection and maintenance of information for recovery and backup purposes is done following NPS Data Center policy and process for backup and retention of information. Disposition of all information is guided by the NPS Records retention schedules for systems that manage information pertaining to natural resources and appropriate risk levels.

There are privacy risks related to hosting, processing and sharing of data, including unauthorized access to records and any inappropriate use and dissemination of information. Privacy risk is very limited due to the data types collected. These risks are mitigated through a combination of physical, administrative, and technical controls, many of which are referenced in the System Security and Privacy Plan. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information.

There is a risk that unauthorized persons could potentially gain access to the limited PII (user logs and, in EQuIS, sample collector, data recorder, and lab name) on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Access to administrative functions is strictly controlled. System administrators periodically review audit logs to prevent unauthorized monitoring. Users are required to accept rules of behavior when using the system. All users must have an account in the system and user authentication protocols are enforced based on the user's role and permissions, i.e. personal identity verification (PIV) cards, two factor authentication, two step verification. Government employees, contractors, and cooperators (collectively, Government Users or DOI PIV credentialed users) will be required to use two-factor authentication. Government Users will be authorized for their role and permissions using a formal process for ensuring least privilege access is maintained before their accounts are created in NR STORET. Government Users will authenticate to NR STORET (EQuIS and Aquarius) using the applicable agency identity provider (e.g. Active Directory Federated Services for DOI) and their DOI issued PIV card.

Transport Layer Security (TLS) technology is employed to protect information in transit using both server authentication and data encryption. Platform and device level encryption have been deployed to encrypt data at rest. Other security mechanisms have

also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

There is a risk that the limited user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes or use of data. Federal employees, contractors, and cooperators are required to take annual mandated security, privacy and records management as well as role-based training where applicable and sign the NPS Rules of Behavior prior to accessing the system. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is a risk that erroneous information may be collected. This risk is mitigated by allowing individuals to access and update only their records in the system. For Government User account, this risk is further mitigated by validating information against DOI Access, authentication results, and activity report and audit log content.

There is a risk that information in the system will be maintained longer than necessary to achieve the agency's mission or may be improperly disposed or destroyed. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Detailed procedures and automated scripts for data disposal/destruction will be developed and secured under change management. Contingency plans and procedures will be defined to ensure the ability to recover in the event of improper data disposal.

There is a risk that individuals providing information do not have adequate notice on how their limited PII will be collected or used. This risk is mitigated by the publication of this PIA.

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:

The log in credentials of the DOI PIV credentialed users are used administratively to track use of the system and changes in the database.

EQuIS' optional sample collector, data recorder, and lab name fields enable the system administrator to contact data contributors should quality assurance/quality control issues manifest themselves.

☐ No

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

☐ Yes

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

Not Applicable.

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:

All users must be DOI PIV credentialed. NR STORET (EQuIS and Aquarius) follows the principle of least privilege. DOI PIV credentialed users are limited to accessing only the data within their assigned park or network (generically known as their 'organization'). Within their organization, users are further constrained based on their role and permission assignments. Some users will have read-only access; some users will have add/edit/delete privileges. Assignment of users to organizations and roles are made by the system administrator when users' request permission to access NR STORET. Assignments are based on least privilege. No one has access to the user audit logs except the system administrator. No one has access to the optional EQuIS sample collector, data recorder, and lab name fields except for the individuals who entered them and the system administrator.

Discrete lab samples, field measurements, and observations from EQuIS system are transmitted to the National Water Quality Monitoring Council's Water Quality Portal (https://www.waterqualitydata.us/) without any PII via an XML file for public dissemination. Continuous data from Aquarius are disseminated via the NPS' AQWebPortal (Aquarius WebPortal: https://irma.nps.gov/aqwebportal/) which is part of the NPS' Integrated Resource Management Applications (IRMA) Portal. No PII (user log in IDs or EQuIS' optional fields) is transmitted to the Water Quality Portal or Aquarius WebPortal.

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

Only DOI PIV credentialed users can access the data in NR STORET. These users have all gone through background checks and login with their PIV cards. Their access is limited to the data in the organization (park or network) they were added to NR STORET to support. Additionally, within their home organization they are assigned roles governing whether they have read-only or add/edit/delete privileges. Only the system administrator has access to all data. The public has read-only access to the water data via the Water Quality Portal (for EQuIS) and Aquarius WebPortal (for Aquarius). No PII

(user log ins or EQuIS' optional fields) is transmitted to the Water Quality Portal or Aquarius WebPortal.

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

EQuIS and Aquarius systems are commercial-off-the-shelf (COTS) software applications and databases for which the NPS pays annual support and maintenance to receive updated versions and technical support. The COTS providers do not have access to the content of the databases.

NPS contractors are involved with the installation and configuration of the software and management of the servers and other network infrastructure. Privacy clauses are included in their contracts. NPS follows AAAP 81 Implementation of Homeland Security Presidential Directive-12 (HSPD-12) at DOI for Contractors and Recipients (Aug 2016).

☐ 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

☒ No

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

☒ Yes

Internal audit logs (date/time stamp, user ID, etc.) record actions taken in the system for security purposes.

The system provides the capability to identify the location where a sample was collected which is incidentally associated with the sample collector's information; however, this information is only used for metadata about the sample collected and is not used for monitoring individuals.

☐ No

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

The location (latitude and longitude) coordinates where the sampler collected the sample is obtained and recorded with the sample collection and incidentally associated with the sample collector's information; however, this information is only used for metadata about the sample collected and is not used for monitoring individuals.

NR STORET uses audit logs, accessible only by a system administrator, to track system performance and user activities. For example, Aquarius' security logs monitor login attempts.

System logging records all attempted access to the NR STORETsystems from users and internal processes, including monitoring, maintenance and audit processes. Items logged include unique identifiers, account names, timestamp, event information, source and successful/unsuccessful login attempts.

At the application/database level, both EQuIS and Aquarius provide some ability to determine who last added/updated records for security purposes. Functionality within the SQL database, if invoked, can track all inserts, updates, and deletes.

As web applications, EQuIS and Aquarius maintain system profiles by log in ID in order to retain the user's software settings and preferences.

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

Access and review of the system/audit logs is strictly limited to the system administrator. Monitoring is a function of the COTS and application system logs which operate behind the scenes in accordance with the system's authorized configurations and programming to ensure the integrity of the data. The system/audit logs are reviewed periodically by the system administrator or upon request by a user if there appears to be an error/discrepancy in the water data. Security anomalies are isolated and investigated to the degree necessary to ensure the continued protection of the system and its data. Additionally, controls have been implemented to prevent unauthorized access by non-authenticated entities and to restrict authenticated users to activities within the scope of their official duties. These controls include access authentication challenges and least privileged permissions architecture. All DOI personnel are required to complete annual security and privacy training and sign DOI Rules of Behavior.

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

Facilities that host NR STORET are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures. Server rooms are locked and accessible only by authorized personnel. Our NPS Denver Data Center has physical environment controls that are identified in their respective SSP.

(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

There are five available levels of electronic security to prevent unauthorized access, which include network access security limits, physical and logical access controls for the Data Center hosting the system, operating system controls, application passwords, and application data group security levels. Access to servers containing system records is limited to authorized personnel with a need to know the information to perform their

official duties and requires a valid username and password. Unique user identification and authentication, such as passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. Access to the system is also limited by network access or security controls such as firewalls, and system data is encrypted using NPS encryption technologies at the hardware level.

(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

All system users are DOI PIV credentialed; have undergone background checks; taken mandatory security, privacy, and records management training; and consented to the rules of behavior. All system users are assigned appropriate roles based on least privilege. Data are encrypted – both in transit and at rest. Nightly backups are performed. The limited PII is only accessible to system administrators or, in the case of EQuIS' sample collector, data recorder, and lab name, the individual who entered it.

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 Water Resource Division's Natural Resource Specialist serves as the Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in NR STORET. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within NR STORET, in consultation with NPS and 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 NR STORET Information System Owner and NR STORET Information System Security Officer are responsible for daily operational oversight and management of the security and privacy controls, for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and appropriate NPS and DOI officials in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the NPS Associate Privacy Officer.

System administrators and contractors are required to report any potential loss or compromise to the Information System Owner and Information System Security Officer.