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: National Indian Oil and Gas Evaluation Management System (NIOGEMS)
Bureau/Office: Assistant Secretary - Indian Affairs, Office of Indian Energy and Economic Development (IEED)
Date: September 27, 2019
Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Road NW, Albuquerque, New Mexico 87104

Section 1. General System Information

A. Is a full PIA required?

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

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

B. What is the purpose of the system?

The Division of Energy and Mineral Development (DEMD) designed and developed the National Indian Oil and Gas Evaluation Management System (NIOGEMS). NIOGEMS is an in-house DEMD-designed major application that uses Geographic Information System (GIS) and relational database off-the-shelf software customized by DEMD for the specific needs of Tribes and supporting DOI offices. NIOGEMS is a mapping-based computer program for maintaining

oil and gas lease, production, and oil and gas well data at Tribal and Bureau resource manager's offices. The system is designed to assist oil and gas producing Indian Tribes to achieve their goals toward self-governance and compacting. Under compacting, Tribal resource managers have readily available access to financial, realty, geo-technical information and complex resources data designed for decision-making on leasing, developing, and managing minerals. NIOGEMS does not collect data; NIOGEMS is used to optimize the data as read-only from other federal systems, which are the system(s) of record for data that is imported into NIOGEMS.

The data-sets imported into the NIOGEMS application for display are from existing DOI systems and commercial sources, which includes: BIA Trust Asset and Accounting Management System (TAAMS), which includes Tribal data; Office of Natural Resources Revenue (ONRR) Minerals Revenue Management Support System (MRMSS), which includes information on managing royalties and resources; Bureau of Land Management (BLM) Legacy Re-host System (LR2000), which includes publicly available information regarding land descriptions and land agreements; Geographic Coordinate Database (GDB) tabular and Geographic Information System (GIS) data; Natural Resources Conservation Service (NRCS) data, National Aerial Imagery Program (NAIP) imagery, CENSUS TIGER GIS data; IHS Energy Well and Production, a commercial data source containing well drilling information and well production information; and other reference spatial data such as roads, streams, lakes, and cities which are made available to authorized NIOGEMS users through a single application. The NIOGEMS system data is provided to Tribal Offices after all non-Tribal PII data has been removed. The NIOGEMS system provides read-only data collected from other systems to assist Tribal and Bureau resource managers. The data is available to the NIOGEMS user in a read-only reference mode and is purged, then replaced with current data on a monthly cycle. Information on individuals is not obtained from publically available record sources.

C. What is the legal authority?

25 U.S.C. §§ 2101-2108, Indian Mineral Development Act of 1982 and 30 U.S.C. §§ 1701-1759, The Federal Oil and Gas Royalty Management Act of 1982

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*

UII Code: 010-000000069, National Indian Oil and Gas Evaluation Management System (NIOGEMS), System Security Plan (SSP), June 25, 2019

☐ 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	Not Applicable	No	Not Applicable

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

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

Records in NIOGEMS are maintained under DOI system of records notices: BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR 68292, November 14, 2014; OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207, March 25, 2016; and LLM-32, Land and Minerals Authorization Tracking System (LR2000), 73 FR 17376, April 1, 2008. These SORNS may be viewed at https://www.doi.gov/privacy/bia_notices.

☐ No

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

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Tribal or Other ID Number
☒ Financial Information

☐ Other: *Specify the PII collected.*

Owner identification number (which contains the Tribal Enrollment Number) assigned to each individual Indian owner and Tract_ID. The TAAMS and MRMSS systems contain additional PII data but NIOGEMS only pulls the PII fields indicated above. The information loaded into NIOGEMS includes both Tribal and individual Indian owners. Individual Indian owner PII data is purged from the NIOGEMS database before it is distributed to Tribal offices. The Tract_ID includes a link that can be used to indicate land included in a reservation. Financial information includes lease terms, such as, bonus bid, royalty rate, rental rate, and duration of primary lease terms.

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*

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

Specified data items are downloaded from the TAAMS and MRMSS systems including PII data. The format of these downloads is an ASCII (man-readable) file. NIOGEMS Data Technicians import the data files, using tools developed for their use, into the NIOGEMS database located on servers accessible only to authorized Technicians.

☐ Other: *Describe*

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

The PII collected and maintained in NIOGEMS is used to assist DOI personnel with managing energy/mineral resources to complete permitting requirements, which is relevant to the purpose of the system.

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.*

NIOGEMS is used to manage reservation oil and gas lease, oil and gas well, production data, and other energy/mineral resources. It allows BIA and other supporting DOI resource managers to readily access financial, realty, geo-technical information and complex resource data gleaned from other data systems/sources, for tracking and making decisions on leasing, developing, and managing energy/mineral resources. After removal of the non-Tribal PII data, the NIOGEMS database is shared with Tribal offices listed below. No other non-DOI offices have access to the NIOGEMS system.

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

Other Bureaus and Offices use the PII collected and maintained in NIOGEMS to manage energy/mineral resources, permitting requirements, and responding to Tribal requests for oil and gas resource information.

☐ 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.*

Tribes are provided information relating to tribal lands, leasing information, and permits. After removal of the non-Tribal PII data, the NIOGEMS database is shared with Tribal offices. No other non-DOI offices have access to the NIOGEMS system.

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

Data is used by contracted NIOGEMS Data Technicians to download data from the source systems, including PII data, and load the data into the NIOGEMS DataBuild database. After completing the DataBuild procedures, the Data Technicians copy the completed databases to the production 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: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ 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.*

Privacy notice is provided through the publication of this privacy impact assessment and the published BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR 68292, November 14, 2014; OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207, March 25, 2016; and LLM-32, Land and Minerals Authorization Tracking System (LR2000), 73 FR 17376, April 1, 2008. These SORNS may be viewed at https://www.doi.gov/privacy/bia_notices.

☐ Other: *Describe each applicable format.*

☐ None

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

Authorized NIOGEMS users are able to retrieve Indian land tract images and data and display them on a map by the owner name, individual owner ID or Indian tract number. For these retrieved tracts, the user is able to display leasing information if the tract has been leased. Conversely, the user can select an Indian tract from a map and display the tract information including Indian owner names and ID.

I. Will reports be produced on individuals?

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

NIOGEMS Data Technicians generate reports, which may include information on individuals; these reports are used to identify owners and their percent ownership. Following the verification process Data Technicians destroy by shredding any reports containing PII.

Reports are produced for individual Tribal members on current oil and gas revenues and future projected oil and gas reserves. The information in the report contains the individual's name and percent ownership for a tract of land.

☐ No

Section 3. Attributes of System Data

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

Data about individuals is not collected from sources other than DOI records. Quarterly, NIOGEMS Data Technicians schedule and select random data items (leases, agreements and wells) from the NIOGEMS database to test for accuracy. A document containing details of each item is printed from the NIOGEMS database and compared to the source data contained in TAAMS, MRMSS, LR2000 and IHS Energy Well and Production databases. Discrepancies in accuracy and completeness are noted in the test reports and corrected. The DEMD NIOGEMS office retains all test result reports but destroys documents containing PII data by shredding.

B. How will data be checked for completeness?

Quarterly, NIOGEMS Data Technicians schedule and select random data items (leases, agreements and wells) from the NIOGEMS database to test for completeness. A document containing details of each item is printed from the NIOGEMS database and compared to the source data contained in TAAMS, MRMSS, LR2000 and IHS Energy Well and Production databases. Discrepancies in completeness are noted in the test reports and corrected. The DEMD NIOGEMS office retains all test result reports but destroys, by shredding, any document containing PII data.

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

The NIOGEMS Data Technicians follow a monthly schedule to update the NIOGEMS DataBuild System with the current source data from BLM LR2000 agreements, TAAMS ownership and leases, and IHS Energy well information and well production. If a data source is unavailable, then the prior month's data is retained and used. Dates that the data was pulled from the source systems are added to the NIOGEMS database and displayed for the users when they log into NIOGEMS. The Data Technicians create a monthly distribution dataset that is copied to the NIOGEMS Production System and the Data Technicians then load the dataset for use by the production users. These procedures are documented in the NIOGEMS documentation library.

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

NIOGEMS records are retained and disposed of in accordance with the Indian Affairs Records Schedule, Series 2200-NIOGEMS, which was approved June 2010 by the National Archives and Records Administration (NARA) under disposition authority N1-075-7-016, and other NARA approved Departmental Records Schedules.

The Master Data File is scheduled as Permanent. A duplicate copy of records is created off-line and physically transferred to the National Archives. Subsequent legal transfer of the records to the National Archives of the United States will be jointly agreed to between the United States Department of Interior and the National Archives.

Printed Report Files are scheduled as Permanent. These records are cut-off at the end of the fiscal year. They are maintained in the office-of-record for 2 years or when no longer needed for current business operations; and then retired to the American Indian Records Repository, a federal records center. Subsequent legal transfer of the records to the National Archives of the United States will be jointly agreed to between the United States Department of Interior and the National Archives.

NIOGEMS temporary records are covered under Department-wide Records Schedule DAA-0048-2013-0001, Item 1.4, Information Technology, which may include short- and long-term records. Records are temporary and are cut-off as instructed in the bureau manual or at the end of the fiscal year in which the files are closed; then destroyed 3 years or 7 years after cut-off depending on the record.

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

Records are disposed of in accordance with the applicable records retention schedule, Departmental policy and NARA guidelines.

Permanent System Records:

Electronic - Prior to archiving, all permanent data, images and system documentation identified, that cannot be printed, within a system will be converted to an acceptable NARA format as required by 36 CFR 1236 and transferred for permanent preservation. Subsequent legal transfer of the records to the National Archives of the United States will be as jointly agreed to between the United States Department of Interior and the National Archives and Records Administration.

Hardcopy - Will be printed and filed by System Report Name, Program, Region, Agency, or Field Office, Job Run Date and Fiscal Year, and cut-off at the end of the fiscal year. Records are maintained in office of record for a maximum of 2 years after cut-off or when no longer

needed for current business operations; and then retired to a records center as approved in the Indian Affairs Records Schedule (IARS). Subsequent legal transfer of the records to the National Archives of the United States will be as jointly agreed to between the United States Department of Interior and the National Archives and Records Administration.

Temporary System records:

NIOGEMS temporary records are covered under Department-wide Records Schedule DAA-0048-2013-0001, Item 1.4, Information Technology, which may include short- and long-term records. Records are temporary and are cut-off as instructed in the bureau manual or at the end of the fiscal year in which the files are closed; then destroyed 3 years or 7 years after cut-off depending on the record.

Copies of records approved for destruction are disposed of by shredding or pulping for paper records, degaussing or erasing for electronic records, in accordance with applicable NARA Guidelines, 384 Department Manual 1, Department and/or Indian Affairs Records Schedules, Indian Affairs Records Management manual, and standard operating policies and procedures.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to the privacy of individuals due to the sensitive PII contained in NIOGEMS. NIOGEMS has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. NIOGEMS is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. To mitigate this risk, access to files is strictly limited to authorized personnel who require access to perform their official duties. In addition to physical controls, operational and technical controls in place to limit these risks include firewalls, encryption, malware identification, and periodic verification of system users. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels are enforced. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; 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 IT Security.

There is also a risk information in NIOGEMS may be used outside the scope of the purpose for which it was collected. This risk is mitigated by access controls implemented to ensure only authorized personnel have access to the information needed to perform official duties and access to NIOGEMS is limited to IEED employees and contractors. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and need-to-know factors, based on the least privilege principle. Access restrictions to data and various parts of the system's functionality is role-based and requires supervisory approval. Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to Sensitive data understand their responsibility to safeguard individual privacy. In addition to physical controls, operational and technical controls in place to limit these risks include firewalls, encryption, malware identification and periodic verification of system users. Firewalls and intrusion detection systems monitor and block unauthorized connections. Current antivirus software is used to check for viruses in real time and logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest, when stored on Federal government owned and operated computer systems with restricted access. Access controls and system logs are reviewed regularly as part of the continuous monitoring process. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets. NIOGEMS has met BIA's information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. This risk is mitigated through monthly updates that require data resolution performed by data technicians. The old data is purged and the new data from TAAMS is loaded. Standard operating procedures (SOP) with detailed checklists have been developed and are used when handling PII in NIOGEMS and when transferring monthly data from the DataBuild environment to the production environment.

There is a risk that individuals may not have notice of the purposes for collecting their information, including how it will be used, or that their PII is sourced from other DOI internal system such as TAAMS, MRMSS, and LR2000. Individuals are notified of the privacy practices through this PIA and through the published DOI SORNs: BIA-04, Trust Asset and Accounting Management System (TAAMS), 79 FR 68292, November 14, 2014; OS-30, Minerals Revenue Management Support System (MRMSS), 81 FR 16207, March 25, 2016; and LLM-32, Land and Minerals Authorization Tracking System (LR2000), 73 FR 17376, April 1, 2008. These SORNS may be viewed at https://www.doi.gov/privacy/bia_notices. This PIA also provides a detailed description of NIOGEMS system sources data elements and how an individual's PII is used.

There is a risk when mailing data to the Tribes. This risk is mitigated by encrypting the data and using a commercial carrier that can track shipments to their destination. Additionally, a log is maintained of all shipments and used to log confirmation that the Tribes received the data. SOP guides with detailed checklists have been developed and are used when handling PII in NIOGEMS and when mailing data to the Tribes.

There is a risk of inadvertently producing Tribal data imports with PII. This risk is mitigated by following procedures and using detailed checklists when producing Tribal data imports, which is documented in multiple SOP guides that cover the transfer of monthly data from the DataBuild environment to the production environment, handling of PII in NIOGEMS, and procedures to load monthly data updates to the production database. The multiple SOP guides provide redundancy in the creation of Tribal data imports.

There may be a risk associated with the collection of information from other DOI systems. NIOGEMS collects data from other internal DOI systems and IEED relies on the accuracy and currency of data, which is the responsibility of each system owner.

There is a risk of creating new data or data aggregation as information in NIOGEMS is obtained from multiple DOI systems, information on individuals is not obtained from publically available record sources. Any risk is mitigated by controls established to limit access to data, using encryption and other safeguards for PII, and limiting the use of PII to that which is necessary to perform official functions related to managing reservation oil and gas leases, well and production values, and other resources.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. In regards to information handling and retention procedures, IEED is responsible for managing and disposing of BIA records in NIOGEMS as the information owner. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. IEED ensures only records needed to support its program, Tribes, and Tribal members is maintained. IEED maintains the records for a maximum of two years or when no longer needed for current business operations, at which time they are transferred to the American Indian Records Repository, a Federal Record Center for permanent safekeeping in accordance with retention schedules approved by NARA under Job Code N1-075-7-016: Series 2200 – NIOGEMS. Information collected and stored within NIOGEMS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

DOI employees must take privacy, Federal Information Systems Security Awareness (FISSA), and records management training before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. 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.

Section 4. PIA Risk Review

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

☒ Yes: *Explanation*

The use of data is both relevant and necessary to the purpose for which the system was designed. Tribal resource managers and DOI offices need access to financial, realty, geo-technical information and complex resource data for management decisions on leasing, developing and managing minerals. NIOGEMS data is used for the purposes of which it was designed, to assist oil and gas producing Indian Tribes to achieve their goals towards self-governance.

☐ 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

The NIOGEMS application does not derive new data about individuals. However, there may be a risk of creating new data or data aggregation as information in NIOGEMS is obtained from multiple DOI systems. Any risk is mitigated by controls established to limit access to data, using encryption and other safeguards for PII, and limiting the use of PII to that which is necessary to perform official functions.

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

☐ Yes: *Explanation*
☒ No

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

☐ Yes: *Explanation*
☒ No

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

Not Applicable. NIOGEMS is not intended to be used in any manner that would allow the system to derive new date or create previously unavailable 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.*

Data is consolidated from TAAMS, MRMSS, LR2000, IHS Energy Well & Production, and other reference spatial data (roads, streams, lakes, cities, etc.). NIOGEMS has physical, technical and administrative controls in place to safeguard the data and protect against unauthorized access or use, loss, or compromise. Access, identification, authentication, and other privacy and security controls follow NIST 800-53 standards and DOI privacy and security policies.

☐ 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*

Users, Contractors, Developers, and System Administrators are given access to NIOGEMS data on a 'least privilege' bases and a need-to-know to perform official functions. Tribal entities that receive Tribal land and well information may have access to the information with non-Tribal PII removed.

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

NIOGEMS users are only given access to data on a 'least privilege' principle and need-to-know based on the individual's role and responsibilities, which requires user's supervisor approval.

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 appropriate Federal Acquisition Regulation Security and Privacy Act Clauses and other security and privacy provisions are in the Contract. Contractors are required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement.

☐ No

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

☐ Yes. *Explanation*
☒ No

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

☐ Yes. *Explanation*
☒ No

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

NIOGEMS Audit Logs collect information on system users such as username, logon date and time, number of failed login attempts, files accessed, user actions or changes to records.

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

NIOGEMS has the ability to audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. NIOGEMS System Administrators will review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. NIOGEMS assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to NIOGEMS Rules of Behavior. Users must complete Federal Information System Security Awareness (FISSA) training, Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled

Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The NIOGEMS audit trail will include system user username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

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 Information System Owner, Information System Security Officer, and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in NIOGEMS. The Information System Owner and the Privacy Act system managers for the related DOI systems are responsible for addressing any Privacy Act complaints and requests access, redress, or amendment of records in consultation with the 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 NIOGEMS Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, 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 NIOGEMS 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, DOI's incident reporting portal, within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with DOI Privacy Officials.