



## 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:** Outer Continental Shelf (OCS) Air Quality System (AQS)

**Bureau/Office:** Bureau of Ocean Energy Management (BOEM)

**Date:** August 28, 2020

**Point of Contact:**

Name: Melissa Allen

Title: BOEM Associate Privacy Officer

Email: boemprivacy@boem.gov

Phone: 202-208-7160

Address: 1849 C Street NW, Washington, DC 20240

### Section 1. General System Information

#### A. Is a full PIA required?

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

No



## **B. What is the purpose of the system?**

The mission of the Bureau of Ocean Energy Management (BOEM) is to manage development of U.S. Outer Continental Shelf (OCS) energy and mineral resources in an environmentally and economically responsible way. Various public laws, rules, and regulations that support BOEM's mission apply to operations on the OCS. Concerning emissions from offshore oil and gas activity, BOEM has regulatory air requirements from the Outer Continental Shelf Lands Act (OCSLA), the Clean Air Act (CAA), and the Consolidated Appropriations Act, 2012 (PL 112-74). The OCSLA authorizes the Secretary of the Interior to prescribe regulations "for compliance with the national ambient air quality standards pursuant to the CAA...to the extent that activities authorized under [this Act] significantly affect the air quality of any State" (43 U.S.C. 1334(a)(8)). The CAA designated to BOEM the OCS air jurisdiction adjacent to Texas, Louisiana, Mississippi, and Alabama. The Consolidated Appropriations Act, 2012 (PL 112-74) effectively transferred jurisdiction to regulate air emissions associated with oil and gas activities adjacent to the North Slope Borough of Alaska from the Environmental Protection Agency (EPA) to BOEM.

BOEM needs methods to accurately account for emissions from offshore oil and gas activity to meet current regulatory air requirements. Photochemical modeling is one way that BOEM assesses air quality impacts from OCS oil and gas sources. Air quality modeling requires emissions inventories as inputs to models. The OCS Air Quality System (AQS) is a Web-based emissions tool that allows operators to submit their activity data to BOEM. Based on that activity data, the OCS AQS calculates monthly and annual emissions, assesses data quality, and provides reports and data visualizations. BOEM will use the emission inventories reports submitted by operators through the OCS AQS as inputs to photochemical modeling to assess oil and gas source impacts to states, as required under the OCSLA. The OCS AQS replaces the Gulf-wide Offshore Activity Data System (GOADS) software, which assisted users in recording information regarding emissions-related offshore activities and generated data files that lessees/operators delivered to BOEM for the calculation of emissions. The OCS AQS improves BOEM's ability to comply with OCSLA requirements and federal mandates to coordinate air pollution control regulations between OCS offshore and states' onshore sources.

## **C. What is the legal authority?**

BOEM derives its authority for requiring emissions monitoring and reporting from the following legal authorities:

- Section 5(a)(8) of the Outer Continental Shelf Lands Act (43 U.S.C. § 1334(a));
- BOEM regulations at 30 CFR 550.303(k) and 550.304(g);
- Consolidated Appropriations Act, 2012 (P.L. 112- 74); and
- Section 328(b) of the Clean Air Act, 42 U.S.C. § 7627(b).



**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

**E. Is this information system registered in CSAM?**

- Yes: 00-06-01-07-02-00 UII code; BOEM OCS AQS System Security and Privacy Plan
- No

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

Subsystem Name	Purpose	Contains PII (Yes/No)	Describe <i>If Yes, provide a description.</i>
None	None	No	N/A

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

- Yes
- No: The OCS AQS is not a system of records. However, login credentials used by Department of the Interior (DOI) and BOEM employees and contractors to access the OCS AQS to perform administration and mission-oriented tasks are covered by the [DOI- 47, HSPD-12: Logical Security Files \(Enterprise Access Control Service/EACS\) SORN](#). Information about the Enterprise Active Directory (EAD) is documented in the Enterprise Hosted Infrastructure PIA available on the [DOI PIA Web page](#).



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

Yes, the information system requires an Office of Management and Budget (OMB) Control Number. OMB has approved current information collection requirements for 1) OMB Control Number 1010-0151—*Air Quality Control, Reporting, and Compliance (30 CFR 550, Subpart B, Plans and Information)*, which has an expiration date of 8/31/2023; and 2) OMB Control Number 1010-0057—*30 CFR Part 550, Subpart C, Pollution Prevention and Control*, which has an expiration date of 5/31/2021.

No

## Section 2. Summary of System Data

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

Name

Other: The purpose of the OCS AQS is to collect and process emissions data from lessees and operators. OCS AQS users include the representatives of lessees/operators submitting emission inventories reports through the system, as well as DOI/BOEM employees and contractors performing administration and mission-oriented tasks.

All new DOI/BOEM and non-DOI users must complete the *OCS AQS User Access Request Form*. The PII that BOEM collects from lessee/operator representatives via the form is limited in nature and includes the non-sensitive, business-related contact information (i.e., email address, phone number, and mailing address) of individuals authorized to submit emissions inventory information on behalf of offshore operators.

Authorized DOI and BOEM employees and contractors access the OCS AQS using their DOI Active Directory (AD) login credentials. The user's name and username data in the OCS AQS is extracted from integration with the DOI EAD system, which authenticates users on the DOI network.

Financial account information related to required payments that lessees/operators make through Pay.gov (e.g., to submit the Conservation Information Document Application for OMB 1010-0151) is processed separately and not maintained in the OCS AQS. Pay.gov is a program of the U.S. Department of the Treasury, Bureau of the Fiscal Service. The Pay.gov PIA is accessible on the [Bureau of the Fiscal Service's PIA Web page](#).



**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: Lessee/operator representatives provide their non-sensitive, business-related contact information to BOEM to facilitate the creation of their OCS AQS access credentials.

**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: All requests for system access must be submitted on the proper *OCS AQS User Access Request Form*, which BOEM will use to add new users, revise existing user access, and deactivate user accounts. Individuals may submit their completed form electronically, but BOEM will not accept access requests submitted in the form of an email note.

DOI and BOEM employees and contractors with Personal Identity Verification (PIV) cards log into the OCS AQS using their DOI AD user credentials. The OCS AQS extracts the name and username of authorized users from system integration with the DOI EAD which authenticates users on the network. Users such as lessee/operator representatives who do not have PIV cards must access the OCS AQS using a username and password.

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

The OCS AQS does not maintain PII beyond user account information used to authenticate users and manage system access. All DOI and non-DOI users requesting access to the OCS AQS must submit a completed *OCS AQS User Access Request Form* to authorize access and facilitate the creation of system access credentials.



BOEM authenticates DOI and BOEM employees and contractors authorized to access the OCS AQS through the DOI EAD. PII for the DOI EAD is collected during the onboarding process.

BOEM uses the non-sensitive, business-related contact information provided by lessee/operator representatives to issue OCS AQS login credentials to individuals authorized to submit data in the system on behalf of a lessee/operator; to provide a point of contact to answer questions or concerns about a company's operations or submitted information; and to implement appropriate system access controls and security monitoring functions.

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

Within the Bureau/Office: Authorized BOEM employees in bureau programs and offices that support balancing the protection and development of OCS resources will have access to emissions inventory data and the contact information of individuals authorized to submit the data on behalf of lessees/operators via the OCS AQS.

Other Bureaus/Offices: BOEM shares emissions inventory data and company-related information (i.e., Company Name, Company Contact Number, and Company Address) with the Bureau of Safety and Environmental Enforcement (BSEE) for compliance purposes.

Other Federal Agencies: BOEM provides the EPA with a copy of the emissions inventory that contains company-related information (i.e., Company Name, Company Contact Number, and Company Address).

Tribal, State or Local Agencies

Contractor: Contractors who provide hosting and Operations & Maintenance support will have access to user PII stored in the OCS AQS.

Other Third Party Sources: BOEM makes publicly available a copy of the database that contains company-related information (i.e., Company Name, Company Contact Number, and Company Address).



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

Yes: Conducting business on the OCS is voluntary. Company representatives may decline to provide information, but in doing so, BOEM may decline to authorize lessee/operator activities.

DOI and BOEM employees and contractors voluntarily provide their information while requesting access to the DOI network and information systems. This normally occurs during the onboarding process and is required to create user accounts in the DOI EAD system and enforce access controls across the DOI network. If users decline to provide the requested information, they will not receive access to the DOI network or DOI information systems (including, but not limited to, the OCS AQS).

No

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

Privacy Act Statement

Privacy Notice: DOI and BOEM employees and contractors can review the [DOI Enterprise Hosted Infrastructure PIA](#) and the [DOI-47, HSPD-12: Logical Security Files \(Enterprise Access Control Service/EACS\) SORN](#) before providing their information to request access to the DOI network and systems.

Before accessing the DOI network and systems, DOI and BOEM employees and contractors are provided with a Privacy Notice that warns of the privacy requirements, consent to monitoring, and references the DOI Privacy Act regulations and applicable Privacy Act penalties when accessing the DOI network.

All individuals requesting access to the OCS AQS can review the Privacy Notice on the *OCS AQS User Access Request Form* before submitting a completed form to BOEM. A warning banner on the OCS AQS login screen provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**WARNING:** This is a United States Department of the Interior computer system. This system is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of the Interior, law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consents to



such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of the authorized site or Department of the Interior personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties under federal laws, including but not limited to Public Laws 83-703 and 99-474. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. DO NOT PROCEED if you do not agree to the conditions stated in this notice.

Other: Notice is provided to all users through this PIA.

BOEM issues a Notice to Lessees and Operators to instruct lessees and operators regarding what production activity information to collect and submit for use in the current OCS Emissions Inventory, as well as where they can find submission instructions for providing the activity reports necessary for compliance with BOEM regulations at 30 CFR 550.303(k) and 550.304(g).

BOEM also provides lessees and operators with Paperwork Reduction Act statements via instructions on BOEM forms related to OMB-approved information collections (1010-0151 and 1010-0057, respectively).

Financial account information related to required payments that lessees/operators make through Pay.gov (e.g., to submit the Conservation Information Document Application for OMB 1010-0151) is processed separately and not maintained in the OCS AQS. Pay.gov is a program of the U.S. Department of the Treasury, Bureau of the Fiscal Service. The Pay.gov PIA is accessible on the [Bureau of the Fiscal Service's PIA Web page](#).

None

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

For typical business use, BOEM does not use any personal identifiers to retrieve records from the OCS AQS. BOEM retrieves records in the system by operator (business) name, complex ID number, structure ID number, or lease number. All activity of a system-level user is recorded and retrievable by system administrators.



## **I. Will reports be produced on individuals?**

Yes: OCS AQS system administrators do not produce reports on individuals, but on the actions of system users. If actions show unusual or malicious behavior, system administrators can use the logs to correlate the actions taken in the system with a username. Only systems administrators and the information system owner will have access to the user activity reports.

No

## **Section 3. Attributes of System Data**

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

BOEM provides instructions to lessees/operators on how to submit activity reports on an annual basis. Lessees/operators are responsible for ensuring that authorized representatives obtain OCS AQS access and submit accurate information to BOEM in accordance with bureau guidance and requirements. Authorized representatives are responsible for the accuracy of the information they provide to BOEM for the creation of their login credentials. BOEM uses the DOI AD to verify the accuracy of login credentials to authenticate the system access of DOI and BOEM employees and contractors.

The OCS AQS performs numerous quality control checks, such as range checks and flags for missing required data, to assist lessees/operators in highlighting potentially incorrect values. If quality control problems remain uncorrected and uncommented upon by the lessees/operators when they submit data, BOEM staff will attempt to reconcile atypical or suspect data by contacting the lessee/operator by email or telephone.

### **B. How will data be checked for completeness?**

Lessees/operators are responsible for submitting complete information to BOEM in accordance with bureau guidance and requirements. Authorized representatives are responsible for the completeness of the information they provide to BOEM for the creation of their login credentials. BOEM uses the DOI AD to authenticate the system access of DOI and BOEM employees and contractors.

The OCS AQS performs numerous quality control checks, such as range checks and flags for missing required data, to assist lessees/operators in entering all required values. If quality control problems remain uncorrected and uncommented upon by the lessees/operators when they submit data, BOEM staff will attempt to reconcile missing data by contacting the lessee/operator by email or telephone.



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

Lessees/operators are responsible for the currency of information they submit to BOEM and are required to inform BOEM if a company official's contact information has changed or another individual has been designated to submit data on their behalf. Lessee/operator representatives are also responsible for updating activity data, as necessary.

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

Records created and stored in the OCS AQS are covered under BOEM Bucket 5 - Regulatory Oversight and Stewardship, approved by the National Archives and Records Administration (NARA) (N1-589-12-5). The Regulatory Oversight and Stewardship business area focuses on ensuring the safe and environmentally sound exploration and production of energy and mineral resources from the OCS. Activities in this business area include: processing plans and permits that ensure work and operational safety and protection of the marine, coastal, and human environments, including implementation of BOEM-mandated mitigations; monitoring industry compliance with laws, rules, and regulations; and providing external technical assistance on oil and gas issues.

The following item number in BOEM Bucket 5 applies to OCS AQS records:

- 5B(5), Environmental Coordination for Site-specific Applications (AAY): All records related to the coordination and consultation with States and other Federal agencies in support of industry submittals [such as Development and Production Plans (DPPs), Development Operations Coordination Documents (DOCDs), Exploration Plans (EPs), pipeline applications, Application for Permit to Modify (APMs), structure removal applications, and G&G applications, and rights-of-use and easements]. Prepare environmental analysis to support the consultations.

Records covered under BOEM Bucket 5B(5) have a temporary disposition and are cut off at close of FY or when activity is completed, retained on-site or at the FRC, and then deleted/destroyed 25 years after cutoff. BOEM does not maintain OCS AQS user PII as part of this collection.

Records on OCS AQS user activity are retained in accordance with DRS – 1, Administrative schedule 1.4 A.1 – [0013] Short Term IT Records – System Maintenance and Use Records (DAA-0048-2013-0001-0013). These records have a temporary disposition. Records are cut-off when obsolete and destroyed no later than 3 years after cut-off.



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

BOEM will maintain PII that is a part of a federal record in accordance with the applicable record retention schedules approved by NARA. 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. Data archive and disposal procedures are outlined in system artifacts. A litigation hold for OCS AQS-related documents will override any records retention schedule or any other DOI/BOEM policy that may otherwise call for the transfer, disposal, or destruction of the relevant documents until the hold has been removed by an authorized authority.

**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 OCS AQS is a Web-based emissions tool that supports BOEM’s mission by enabling lessees and operators to submit their activity data to BOEM. BOEM will use these submitted emission inventories reports to assess oil and gas source impacts to states to comply with OCSLA requirements and Congressional mandates to coordinate air pollution control regulations between OCS offshore and states’ onshore sources.

BOEM manages and safeguards U.S. Government systems and information in accordance with the Federal Information Security Modernization Act (FISMA), OMB policies, National Institute of Standards and Technology (NIST) standards, and DOI security and privacy policies. BOEM use of the OCS AQS poses minimal risks to the privacy of individuals, as the system neither collects nor maintains sensitive PII or personal information. The OCS AQS uses the principle of least privilege access for authorized users to submit and manage activity data. OCS AQS users are either lessee/operator representatives or DOI and BOEM employees and contractors. All OCS AQS users must complete the *OCS AQS User Access Request Form*. DOI/BOEM users must complete required training (security and privacy awareness training, as well as role-based training) and sign the DOI Rules of Behavior before being granted access to the system and annually thereafter.

Internal OCS AQS access is controlled by information from the DOI EAD that is shared with the OCS AQS for the purpose of authenticating internal users and managing their access. Users representing BOEM-qualified companies can input, modify, and view data for their companies only by logging into the OCS AQS using their BOEM-approved accounts. Companies and the supervisors of BOEM OCS AQS users are required to promptly request account updates such as user changes or account deactivations, as necessary. BOEM (at least) annually reviews user access in accordance with OCS AQS account management procedures.



BOEM provides adequate notice to the authorized representatives of companies. BOEM's collection of information from lessees/operators is covered under several applicable OMB-approved information collections. BOEM also issues a Notice to Lessees and Operators to instruct lessees and operators regarding what activity information to collect and submit for use in the current OCS Emissions Inventory and where they can find submission instructions for providing the activity and emissions reports necessary for compliance with BOEM regulations. Financial account information related to required payments that lessees/operators make through Pay.gov (e.g., to submit the Conservation Information Document Application for OMB 1010-0151) is processed separately and not maintained in the OCS AQS. Pay.gov is a program of the U.S. Department of the Treasury, Bureau of the Fiscal Service (BFS). The BFS provides notice to Pay.gov users through the Pay.gov PIA that users can access on the [Bureau of the Fiscal Service's PIA Web page](#).

The OCS AQS is not a Privacy Act system of records subject to accounting of disclosures, but security and privacy controls are in place to limit access to user PII and activity data to personnel who have a verified need to access the information. The OCS AQS login page reminds users of their responsibilities by displaying a warning banner, which informs users that they have no explicit or implicit expectation of privacy. Beyond DOI, other federal agencies will not have direct access to the system. However, BOEM is authorized to share PII (i.e., company contact information) and data with BSEE and the EPA, as necessary.

BOEM use of DOI information and information technology (IT) systems is conducted in accordance with the appropriate DOI use policy. The OCS AQS will maintain an audit trail of activity sufficient 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. Only system administrators and the information system owner will have access to system reports. System administrators review audit logs on a regular, periodic basis and immediately report any suspected attempts of unauthorized access or scanning of the system to IT Security. The OCS AQS follows DOI-Office of the Chief Information Officer guidelines in that accounts are automatically locked after 45 days of inactivity. Users are responsible for keeping their accounts active. When the OCS AQS reaches the end of its life, the equipment and/or media that contains users' names, system usernames, and audit logs will be retained per the retention schedule for IT systems and then destroyed. BOEM programs maintain operator and emissions information in accordance with current identified recordkeeping schedules and any existing litigation holds. BOEM does not maintain OCS AQS user PII while maintaining applicable records under item 5B(5) of BOEM Bucket 5 - Regulatory Oversight and Stewardship. OCS AQS user activity data is maintained under a short-term schedule, which mitigates privacy risk.



## 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: Data that BOEM collects through the OCS AQS supports the bureau's mission to manage development of U.S. OCS energy and mineral resources in an environmentally and economically responsible way. The PII that BOEM collects from OCS AQS users facilitates the creation of their system credentials. System credentials are required to facilitate storage and retrieval of user-created content and data, as well as to implement access controls. BOEM will use the submitted emission inventories reports to assess oil and gas source impacts to states, as required under the OCSLA and other legal authorities. Submission of the information is required under OMB Control Numbers 1010-0151 and 1010-0057, respectively.

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. The OCS AQS does not derive new data about individuals.



**F. Are the data or the processes being consolidated?**

- Yes, data is being consolidated.
- Yes, processes are being consolidated.
- 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: Lessee/operator representatives will only have access to information concerning their respective companies.

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

The OCS AQS uses the principle of least privilege access for authorized users to perform duties as defined by assigned roles. All DOI and non-DOI users must complete the *OCS AQS User Access Request Form*. The OCS AQS Account Manager will create, modify, disable, and terminate system accounts in accordance with OCS AQS account management procedures.

Access to data for DOI and BOEM users is restricted through AD permissions and access controls. Separated employees are also removed from AD, which effectively removes their access to the DOI network and the OCS AQS. Only systems administrators will have access to OCS AQS audit log data.

To manage the access of representatives of lessees/operators, BOEM reviews submitted access request forms against the official company records on file. Company representatives are restricted to editing and viewing their own company's data.

**I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?**

- Yes. Applicable Privacy Act contract clauses are included in the contract.
- 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. In accordance with NIST 800-53 controls, audits logs that identify all users and actions associated with their usernames are maintained in the OCS AQS. When a user logs in and navigates through the system, their username and name will be captured in system audit logs. System logs provide a chronological record of information system activities.

No

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

All activity of a system-level user is recorded. Usernames can be associated with any of the following events and are captured in the OCS AQS audit logs: successful and unsuccessful account logon events, account management events, object access, policy changes, privilege functions, process tracking, system events, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.

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

BOEM complies with NIST and other federal requirements for data security as part of a formal program of assessment and authorization, as well as continuous monitoring. The OCS AQS 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 and can perform tasks as defined by their assigned roles.

The OCS AQS maintains an audit trail of activity sufficient to reconstruct relevant security events. Only authorized users with system administrator privileges have access to monitor users' activities in the system. System administrators review audit logs on a regular basis and immediately report any suspected attempts of unauthorized access or scanning of the system 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

(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

(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



**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 OCS AQS Information System Owner is responsible for the overall oversight and management of security and privacy controls. The OCS AQS Information System Owner and the OCS AQS Information System Security Officer are responsible for ensuring the implementation of adequate safeguards to protect individual privacy and agency data in compliance with federal laws and policies for the data managed and stored in the system. The OCS AQS is not a system of records. The BOEM Associate Privacy Officer will coordinate with the OCS AQS Information System Owner and other appropriate officials to address any reported privacy complaints or concerns.

**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 OCS AQS Information System Owner is responsible for the overall oversight and management of the system's security and privacy controls, as well as for ensuring the proper management of data and the granting of access to agency data in a secure and auditable manner. The OCS AQS Information System Owner and the OCS AQS Information System Security Officer are responsible for reporting any loss, compromise, unauthorized disclosure, or unauthorized access to PII and agency data to DOI-CIRC and appropriate officials in accordance with federal policy and established procedures, including but not limited to, the DOI Privacy Breach Response Plan.