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 Air Quality System (OCS AQS)
Bureau/Office: Bureau of Ocean Energy Management (BOEM)
Date: September 30, 2023
Point of Contact
Name: Melissa Allen
Title: BOEM Associate Privacy Officer
Email: boemprivacy@boem.gov
Phone: 571-474-7967
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?

BOEM’s mission is to manage the development of U.S. Outer Continental Shelf (OCS) energy and mineral resources in an environmentally and economically responsible way. 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 U.S. 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 (OCS AQS) is a comprehensive Web-based software solution for managing and reporting OCS emission source data in the Gulf of Mexico and Alaska regions. 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.

The OCS AQS replaced the Gulfwide Offshore Activities 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's authority for requiring emissions monitoring and reporting is based on section 5(a)(8) of the OCSLA, 43 U.S.C. § 1334(a)(8), (the geographical extent of which was modified by the Consolidated Appropriations Act, 2012 (P.L. 112-74)), and BOEM's regulations at 30 CFR 550.303(k) and 550.304(g).

The U.S. General Services Administration (GSA) developed Login.gov pursuant to 6 U.S.C § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 U.S.C § 501.

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 the Governance, Risk, and Compliance platform?

☒ 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** *If Yes, provide a description.*
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 does not create a system of records. However, records related to login credentials used by Department of the Interior (DOI) and BOEM employees and contractors to access the OCS AQS are covered by INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) – 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021). Information about Enterprise Directory Services is documented in the Enterprise Hosted Infrastructure (EHI) PIA available for review on the DOI PIA Web page.

GSA owns and operates Login.gov, a single, secure platform through which members of the public can sign in and access information and services from participating federal agencies. Lessee/operator representatives securely log into OCS AQS through authentication provided by Login.gov. GSA maintains records on individuals who utilize Login.gov and has published a SORN for the Login.gov system, GSA/TTS–1 (Login.gov), 87 FR 223 (November 21, 2022). The SORN is available for review on the GSA SORNs Web page.

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

☒ Yes: OMB has approved current information collection requirements for OMB Control Number 1010-0057—*30 CFR Part 550, Subpart C, Pollution Prevention and Control*, which has an expiration date of 3/31/2024.

☐ 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 inventory 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 and BOEM employees and contractors performing administration and mission-oriented tasks.

Lessee/operator representatives provide their non-sensitive, business-related contact information (i.e., email address, phone number, and mailing address) to BOEM to submit emissions inventory information on behalf of offshore operators. BOEM or the Bureau of Safety and Environmental Enforcement (BSEE) (BSEE uses OCS AQS data for inspection purposes and provides BOEM with information technology services) will send an invitation email to lessee/operator representatives on file with instructions on how to access the OCS AQS. Lessee/operator representatives may also send an account request to the OCS AQS Support Team if they did not receive an invitation. Consultants hired by an operator to complete the inventory will need the operator to request an account on their behalf; operators should submit their requests to the OCS AQS Support Team.

To log into the OCS AQS, lessee/operator representatives (including consultants) approved by BOEM for system access must create a Login.gov account using the same email address through which they received their OCS AQS invitation from BOEM or BSEE. (To use a different email address to log into the OCS AQS, lessee/operator representatives must send a request to the OCS AQS Support Team.) Authentication provides BOEM with minimal assurance that the same individual who created the Login.gov account is accessing the OCS AQS. For authentication to establish a secure account, GSA requires a name, email address, and an authentication method (e.g., a phone number where GSA will share a Short Messaging Service code, Universal Serial Bus Security Key, or other options). By creating a Login.gov account to log into the OCS AQS, lessee/operator representatives are consenting for GSA to share their PII (i.e., email address and the Universally Unique Identification Number (UUID) assigned by GSA to that user) with BOEM for the purpose of user authentication. Refer to the GSA Login.gov PIA for information on how user PII data is collected, used, stored, and disseminated by GSA's Login.gov service.

Authorized DOI, BSEE, and BOEM employees and contractors access the OCS AQS using their DOI Active Directory (AD) login credentials. PII for the DOI AD (i.e., username, password hash values, HSPD-12 authentication, official email address and phone number, duty station address, official title, and other categories described in the EHI PIA) is collected during the onboarding process.

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 must create a Login.gov account using the same email address through which they received their invitation from BOEM or BSEE to log into the OCS AQS. Consultants hired by an operator to complete the inventory will need the operator to request an account on their behalf. By creating a Login.gov account and using it to access the OCS AQS, lessee/operator representatives (including consultants) are consenting for GSA to share their PII with BOEM for the purpose of user authentication.

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: Lessee/operator representatives will receive an email invitation from BOEM or BSEE to initiate the OCS AQS account creation process. All requests to setup, modify, or deactivate system access must be submitted to BOEM in accordance with current established procedures. Individuals may submit their completed form electronically.

GSA Login.gov collects information directly from lessee/operator representatives who create Login.gov accounts. Login.gov acts as an identity credential provider for BOEM to verify the identity of external (i.e., non-DOI) OCS AQS users.

DOI, BSEE, and BOEM employees and contractors with Personal Identity Verification (PIV) cards log into the OCS AQS using their DOI AD login credentials. The AD continuously updates data across the DOI domains.

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

All lessee/operator representatives who require access to the OCS AQS must follow current established procedures to facilitate the creation of their system access credentials. The OCS AQS is not intended to maintain PII beyond user account information used to authenticate users, implement appropriate system access controls, and manage security monitoring functions.

BOEM authenticates DOI, BSEE, and BOEM employees and contractors authorized to access the OCS AQS through the DOI AD. Lessee/operator representatives must have a user account (authenticated through Login.gov) to submit a company's emission inventory data through the OCS AQS.

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: BSEE works in coordination with BOEM to provide environmental oversight in areas where DOI has authority to regulate air emissions from offshore oil and gas and renewable energy operations. BOEM shares emissions inventory data and company-related information (i.e., Company Name, Company Contact Number, and Company Address) with BSEE for regulatory compliance purposes. BSEE conducts inspections based on OCS AQS data.

☒ Other Federal Agencies: A formal Interagency Agreement is executed between Login.gov and BOEM before any information is shared for user authentication purposes. Login.gov will share an external OCS AQS user's information with BOEM for user authentication purposes with the user's consent; the user must enter their password to provide that consent.

The EPA's electronic Greenhouse Gas Reporting Tool (e-GGRT) supports facility and supplier reporting for the USEPA Greenhouse Gas Reporting Program (GHGRP). OCS AQS contains a tool capable of generating an e-GGRT file in the appropriate XML format for submission to USEPA for a single facility or a complex with multiple facilities. Operators that fall under the reporting requirement can easily generate an e-GGRT-formatted XML report using the provided inputs. 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.

OCS AQS technical support is available to system users during normal workdays. OCS AQS Support Team contractors will use the information shared by lessee/operator representatives to address their expressed issues.

☒ Other Third Party Sources: In accordance with 76 FR 64431, BOEM will make data and information available in accordance with the requirements and subject to the limitations of the Freedom of Information Act (FOIA) (5 U.S.C. 552). BOEM makes publicly available a copy of the database that contains company-related information (i.e., Company Name, Company Contact Number, and Company Address).

The GSA Login.gov service may share PII provided by individuals with contracted third party organizations for identity verification and authentication purposes. Review the Login.gov PIA for details on how PII data is shared with third party entities.

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

☒ Yes: DOI, BSEE, and BOEM employees and contractors voluntarily provide their information while requesting access to the DOI network and information systems. Users can consent during the onboarding process and verification of approval to work is required to enforce access controls across the DOI network. If users decline to provide the required information upon employment at DOI, they will not be given access to the network or DOI information systems (including, but not limited to, the OCS AQS) and may be unable to perform their duties.

Conducting business on the OCS is voluntary. Lessee/operator representatives must opt in to share information with BOEM through Login.gov. They may decline to provide their information to BOEM and Login.gov, but in doing so, the bureau may decline to authorize lessee/operator activities and cannot authorize OCS AQS access. GSA has published a SORN and PIA for Login.gov. The Login.gov website has clear detailed instructions on the steps and PII involved with establishing a user account and provides a detailed Login.gov Privacy Act statement that describes the authority, purpose, routine uses, and consent mechanism.

☐ No

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

☒ Privacy Act Statement: Lessee/operator representatives can review the Privacy Act Statement that Login.gov provides to individuals who are creating an account or signing in using Login.gov.

DOI, BSEE, and BOEM employees and contractors are provided a Privacy Act Statement during the onboarding process when they are providing information for the issuance of PIV credentials.

☒ Privacy Notice: All individuals requesting access to the OCS AQS can review the *OCS AQS User Access Request Form* and *Rules of Behavior* before submitting a completed form to BOEM.

DOI, BSEE, and BOEM employees and contractors can review the DOI Enterprise Hosted Infrastructure PIA, DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control

Service/EACS) SORN, and a Privacy Act Statement provided in DOIAccess before providing their information to request access to the DOI network and systems. The PIA and SORN are available for review on the DOI PIA Web page and DOI-wide SORNs Web page.

Lessee/operator representatives can review the GSA Login.gov PIA and GSA/TTS-1, Login.gov SORN before providing their information to GSA to create a Login.gov account for details on the specific collection, use, storage or sharing of their PII by GSA.

BOEM also provides notice through the publication of this PIA on the DOI PIA Web page.

☒ Other: A warning banner on the OCS AQS login screen provides all system users with privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

A link to the Login.gov Security Practices and Privacy Act Statement page is available to lessee/operator representatives when they create an account or sign in using Login.gov. A link to the website Privacy Policy is also accessible in the footer of the OCS AQS Login.gov page. BOEM issues a Notice to Lessees and Operators to instruct them about the activity information and related emissions source data they should collect and submit to the bureau for the OCS Emissions Inventory, as well as to inform them about where they can find instructions for submitting the activity and emissions reports necessary for compliance with BOEM's regulations at 30 CFR 550.303(k) and 550.304(g).

A Paperwork Reduction Act Statement that displays the current and valid OMB Control Number is available for review on the OCS AQS login screen and reiterates information presented in the Notice to Lessees and Operators.

Before accessing the DOI network and systems, DOI, BSEE, and BOEM employees and contractors are provided with a DOI Security Warning Banner that informs them they are accessing a DOI system, they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

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

BOEM typically does not use any personal identifiers to retrieve data from the OCS AQS. BOEM retrieves records in the system by operator (company) name, complex identification (ID) number, structure ID number, or lease number.

I. Will reports be produced on individuals?

☒ Yes: All activity of a system-level user is recorded and retrievable by system administrators. OCS AQS system administrators can produce reports 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. Audit logs show the list of users who accessed the system and the types of activities performed such as logins, logoffs, project selections, etc.

The GSA Login.gov service may produce compliance/audit reports on individuals' actions in the system for investigatory and fraud mitigation purposes. Review the GSA Login.gov PIA for information on reporting functions within the system and how reports on individuals are generated, used, or shared.

☐ 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. Lessee/operator representatives are responsible for submitting accurate emissions inventory information to BOEM in accordance with bureau guidance and requirements. The OCS AQS assists lessees/operators by performing numerous quality control checks, such as range checks and flags for missing required data, to highlight potentially incorrect values. If the Quality Assurance/Quality Check (QA/QC) finds no errors, an email will be sent to the BOEM reviewer and operator submitting the report that the submission was accomplished. BOEM staff will attempt to reconcile atypical or suspect data by contacting the submitter by email or telephone.

BOEM uses DOI AD user account information to authenticate user access and actions. This information is constantly synchronized through interface with AD.

Lessee/operator representatives are responsible for the accuracy of the information they provide to BOEM and Login.gov for the creation of their login credentials and user authentication. Lessee/operator representatives must have accurate information on-file to receive an invitation from BOEM or BSEE to access the OCS AQS. Consultants hired by an operator to complete the inventory will need the operator to request an account on their behalf.

When setting up a Login.gov account to authenticate OCS AQS access, lessee/operator representatives must use the same email address at which they received the OCS AQS invitation from BOEM or BSEE. They must send a request to the OCS AQS Support Team if they would like to use a different email address. Login.gov ensures the accuracy and completeness of the user's email address and phone number (if provided for multi-factor authentication) by requiring the user to confirm their email address and entering the one-time security code provided to them. OCS AQS users who use the Login.gov service can review the GSA Login.gov PIA for information on how their PII is verified for accuracy.

B. How will data be checked for completeness?

Lessee/operator representatives are responsible for submitting complete information to BOEM and Login.gov to facilitate the creation and authentication of their OCS AQS account. BOEM uses the DOI AD to authenticate the system access of DOI, BSEE, and BOEM employees and contractors who must provide the bureau with accurate information regarding their OCS AQS access requirements.

The OCS AQS contains mechanisms to perform QA/QC checks, such as range checks and flags for missing required data, to assist lessees/operators in entering all required values. BOEM will review source inventories after submission. If there are questions regarding the inventory data, BOEM may send an inventory back with comments for corrective action and resubmission. To further assist in BOEM's completeness checks, the bureau requires an OCS AQS report submittal even if a structure is out of service during the entire reporting year.

GSA verifies the PII data provided by lessee/operator representatives for Login.gov user accounts. Lessee/operator representatives must ensure that the contact information they have provided for account creation are accurate, complete, and accessible to them. OCS AQS users who use Login.gov to access the system can review the GSA Login.gov PIA for information on how their PII is checked for completeness.

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

Procedures for data submissions are detailed in published Notices to Lessees and Operators, OCS AQS Frequently Asked Questions, and the OCS AQS User Manual. Lessees/operators are responsible for the currency of information they submit to BOEM and are required to inform BOEM of any changes to their contact information or access needs in a timely manner.

Login.gov collects PII directly from the individuals using GSA's identity authentication and verification service to access the OCS AQS. Therefore, the PII is presumed to be current at the time that it is provided by the individuals. The Login.gov account page allows a user to update or amend any PII in the system used for account authentication following established procedures. Lessee/operator representatives must use the same email address in which they received an OCS AQS invitation to create a Login.gov account. Lessee/operator representatives who would like to use a different email address must contact the OCS AQS Support Team. OCS AQS users who use the Login.gov service to access the system can review the GSA Login.gov PIA for information on how their PII data is kept current.

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

OCS AQS records 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.

The OCS AQS keeps copies of all files imported, exported, and generated by the system. Records covered under BOEM Bucket 5B(5) have a temporary disposition and are cut off at the close of the fiscal year or when the activity is completed, retained on-site or at the Federal Records Center, and then deleted/destroyed 25 years after the cut off.

Information Technology records are maintained under Departmental Records Schedule (DRS) 1 - Administrative Records, which was approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-001). DRS-1.4, Information Technology, covers records that document the Department's creation, management, and use of IT systems and applications, system design and implementation, change management, technological specifications, system security files, maintenance and monitoring records, system documentation, risk management, and all related forms and documents for managing electronic systems. Retention periods vary as records are maintained in accordance with the records schedule for each specific type of record. Routine short-term IT records related to system maintenance and use that are not needed for extended retention have a temporary disposition. Records are cut off when superseded or obsolete, and destroyed no later than 3 years after cut-off, unless longer retention is required for administrative, legal, audit, or other operational purposes.

GSA is responsible for managing its Login.gov records in accordance with the Federal Records Act and approved records retention schedules. Please refer to the Login.gov PIA for information on the retention of Login.gov records.

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

BOEM maintains records in accordance with the applicable record retention schedules approved by NARA. Data archive and disposal procedures are outlined in system artifacts. Approved disposition methods include shredding or pulping for paper records and degaussing or erasing for electronic records in accordance with NARA Guidelines and Departmental policy.

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.

BOEM does not use the OCS AQS to collect and maintain any PII apart from that used to create and manage system accounts. Therefore, the OCS AQS poses limited privacy risks to internal and external users. BOEM and its service providers mitigate these limited privacy risks through the implementation of a combination of administrative, technical, and physical controls.

The OCS AQS has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. The OCS AQS is rated as a FISMA Moderate impact system and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the data contained in the system. The OCS AQS System Security and Privacy Plan is based on NIST guidance and is part of a continuous monitoring program that includes ongoing security and privacy control assessments to ensure appropriate security and privacy controls have been implemented to prevent the unauthorized access, use, or disclosure of records maintained in the OCS AQS in accordance with Federal laws, regulations, and policy.

BOEM uses the privacy assessment process to determine privacy risks and take steps to mitigate them, as appropriate. There are risks that BOEM will collect information without authorization, collect more information than necessary to fulfill a business purpose, and provide inadequate notices to OCS AQS users regarding applicable privacy practices. BOEM is authorized by several legal authorities to collect information through the OCS AQS to facilitate the participation by the offshore operators in the bureau's annual survey program. BOEM notifies OCS AQS users of the applicable legal authorities through this PIA and published Notices to Lessees and Operators. BOEM also complies with the Paperwork Reduction Act by obtaining OMB approval for the collection of emissions inventory data and displaying a currently valid OMB Control Number at the point of collection.

A warning banner on the OCS AQS login screen provides all system users with privacy and security notices consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. BOEM also provides a general privacy notice to all OCS AQS users through the publication of this PIA. For DOI, BSEE, and BOEM employees and contractors whose system access is authenticated through the DOI AD, notice is also provided through the DOI Enterprise Hosted Infrastructure PIA, INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) SORN, and a Privacy Act Statement provided in DOIAccess. Lessee/operator representatives provide their contact information to BOEM when requesting the creation of an OCS AQS user account and must create a Login.gov account for authentication purposes. Before providing their information to GSA to create a

Login.gov account, lessee/operator representatives may review the Login.gov Privacy Act Statement, PIA, website Privacy Policy, and the GSA/TTS-1, Login.gov SORN. By accessing the Login.gov service to authenticate their access to the OCS AQS, operators and authorized consultants are acknowledging and agreeing to the Login.gov Privacy Policy and the Login.gov Rules of Use. Individuals may request access to or amendment of their records by following the procedures outlined in the applicable SORNs. OCS AQS users may also contact DOI or BOEM Privacy Officials with any questions or privacy concerns.

There is a risk that unauthorized persons could potentially gain access to the OCS AQS. The OCS AQS login screen warns users that any unauthorized use of or access to the OCS AQS may subject violators to criminal prosecution and penalties. To further reduce the risks of unauthorized system access and use, BOEM approves access and assigns OCS AQS access roles, authenticates user access through the DOI AD (internal users such as DOI, BSEE, and BOEM employees and contractors) and Login.gov (external users such as lessee/operator representatives), and reviews audit logs. BOEM collects the minimal amount of user information to create and manage user accounts and assigns roles and privileges to approved users based on the least privilege principle. External users are authenticated through Login.gov and internal users are authenticated through the DOI AD. The OCS AQS has the functionality to audit user activities and maintains an audit log of activity sufficient to reconstruct security-relevant 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. Computer servers on which electronic records are stored are in secured DOI facilities with physical, technical, and administrative levels of security to prevent unauthorized access to the DOI network and information systems. Security controls to protect the DOI network and information systems include encryption, firewalls, audit logs, and network system security monitoring.

A formal Interagency Agreement is executed between Login.gov and BOEM before any information is shared for user authentication. GSA has completed a System Security and Privacy Plan for Login.gov, which is designated as a FISMA Moderate impact system and has a GSA-issued FedRAMP authority to operate in place. Login.gov data is encrypted both in transit and at rest. Login.gov audits access, enforces training requirements, vets privileged users, and enforces the principles of least-privileged access to reduce the risks of unauthorized system access and use. By keeping all audit logs for any action taken as a privileged user on Login.gov systems, there is a detailed history maintained to determine who made changes and when. All GSA personnel are trained on how to identify and safeguard PII. In addition, each employee must complete annual privacy and security training. Those who need to access, use, or share PII as part of their regular responsibilities are required to complete additional role-based training. By using background check investigations for privileged users, Login.gov seeks to grant access only to those who exhibit a high level of trustworthiness. By maintaining least-privileged access, Login.gov restricts access to the minimum required levels, decreasing the risk of unauthorized disclosure or abuse. Login.gov also leverages third-party services to confirm device integrity, characteristics, reputation, and association with individual; validate behavioral analytics; confirm Internet Protocol address and email reputation; and protect against synthetic identities (false identities created by fraudulent actors). These services are embedded into Login.gov's authentication and identity verification services.

All DOI, BSEE, and BOEM employees and contractors must complete Information Management Technology (IMT) Awareness Training and the Information Systems Security Rules of Behavior Acknowledgment before acquiring network and/or system access and annually thereafter. IMT Awareness Training includes modules on Cybersecurity - Federal Information Systems Security Awareness (FISSA), Privacy Awareness, Records Management, Section 508 Compliance, Controlled Unclassified Information (CUI), and the Paperwork Reduction Act. Personnel with significant privacy and security responsibilities must also complete role-based training before acquiring network and/or system access and annually thereafter. Role-based privacy training requirements are in accordance with OMB Circular A-130, NIST guidance, and DOI Security and Privacy Control Standards. Role-based security training requirements are in accordance with 5 CFR § 930.301 (2004), the FISMA, OMB Circular A-130, NIST guidance, and DOI Security and Privacy Control Standards.

In accordance with 76 FR 64431, BOEM will make data and information available in accordance with the requirements and subject to the limitations of the FOIA (5 U.S.C. 552). BOEM makes publicly available a copy of the database that contains company-related information (i.e., Company Name, Company Contact Number, and Company Address). BOEM must review information before disseminating it to the public to prevent the unauthorized disclosure of sensitive or privileged information. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, and criminal, civil, and administrative penalties. DOI, BSEE, and BOEM employees and contractors are required to report any suspected or confirmed incident to DOI-CIRC, DOI's central incident reporting portal, within 1-hour of discovery in accordance with Federal policy and procedures. For any suspected or confirmed privacy breach, the DOI Privacy Breach Response Plan will be implemented by the BOEM APO.

There is a risk that data may be stored in the OCS AQS longer than necessary, which is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. The emissions data stored in the OCS AQS do not contain PII. OCS AQS records are maintained and disposed of under a NARA-approved records schedule. BOEM collects and uses only the minimum amount of PII needed to authenticate users and manage system access. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act, NARA guidelines, and Departmental policy. DOI, BSEE, and BOEM employees and contractors also must complete records management training (as part of IMT Awareness Training) to reinforce the requirements to maintain, protect, and dispose of records (including those collected and stored in the OCS AQS) in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

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: OCS AQS users provide their non-sensitive, business-related contact information to BOEM (and Login.gov, if they are external users) to facilitate the creation of their login credentials. BOEM needs the emissions inventory information that lessee/operator representatives submit through the OCS AQS to evaluate the effectiveness of its regulations under § 5(a)(8) of the OCSLA, 43 U.S.C. § 1334(a)(8) and to support BOEM's environmental analyses and coordination with other agencies. The 1990 CAA Amendments (Pub. L. No. 101-549, Nov. 15, 1990) require states to prepare air emission inventories every three years (beginning in 1996). BOEM has assisted states and the EPA with meeting this requirement by collecting and compiling emissions from OCS sources. These emission inventories support the coordination between DOI and the EPA called for in § 328(b) of the CAA (42 U.S.C. § 7627(b)) with respect to regulation of OCS emissions in areas under DOI air quality jurisdiction and emissions in adjacent onshore areas.

☐ No

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

☐ Yes

☒ No: The GSA Login.gov system aggregates information required to protect it from unauthorized use. Please refer to the Login.gov PIA for information on how user data is aggregated and used.

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?

The OCS AQS does not derive new data about individuals.

The OCS AQS contains mechanisms for conducting QA/QC checks on input emissions inventory data. Lessee/operator representatives must correct all highlighted errors before they can submit an emissions inventory report to BOEM. If the QA/QC finds no errors, an email will be sent to the BOEM reviewer and the lessee/operator representative submitting the report that the submission was accomplished.

Once all facilities in the inventory have been submitted by a user, the inventory will be locked so that no additional changes can be made. BOEM will review the submittal and either accept it or send a notification back to the operator that additional action must be taken before it can be accepted. Notification will be sent via email and messaging within OCS AQS. The inventory will be unlocked when additional action is required so the necessary changes can be made to the data for the facility in question.

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. The OCS AQS Support Team provides tech support to users on behalf of the system developer.

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.

OCS AQS users have read-only access to all facilities for past, final inventories that are publicly available.

Lessee/operator representatives will only have access to information regarding their specific inventories and facilities. OCS AQS comes with a set of report functions that can be customized by the operator using OCS AQS Reports wizards to produce a variety of summary and analysis reports. These reports can then be printed or exported into an external format for ease of distribution.

Company representatives are restricted to editing and viewing their own company's data. Access to data for DOI, BSEE, and BOEM users is restricted through AD permissions and access controls based on their need-to-know. Separated employees are removed from AD, which effectively removes their access to the DOI network and the OCS AQS.

Only system administrators will have access to OCS AQS audit log data and the OCS AQS Admin Module.

GSA Login.gov privileged users may have access to view data supplied by individuals to GSA for their user accounts and for identification verification and authentication but cannot amend or delete PII data within a record. GSA does not have access to the OCS AQS.

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

☒ No: Privacy Act contract clauses were not included in the contract. The OCS AQS is not a Privacy Act system. BOEM will work with contracting officials to include the appropriate privacy clauses and terms and conditions.

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. Audit logs that identify all users and actions associated with their usernames are maintained in the OCS AQS. System logs provide a chronological record of OCS AQS user activities.

For GSA Login.gov, all user actions are logged and monitored including metrics that track and measure user behavior and engagement with the Login.gov system. Privileged users' actions on the system are monitored, logged, and reviewed due to the required additional safeguards and controls around their actions. Users who opt to utilize the GSA Login.gov service may view the

Login.gov website policy and PIA for additional information.

☐ No

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

All OCS AQS user activities are 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.

All Login.gov traffic is subject to monitoring and recording to identify unauthorized attempts to change information; jeopardize the confidentiality, integrity, or availability of Login.gov; or otherwise cause damage. Information included in security reports may include IP addresses, master and agency universally unique identifiers, and user agents (i.e., browsers) that access Login.gov. Login.gov system administrators and security personnel can generate user activity reports based on any combination of analytics attributes that are tracked to investigate potential incidents, diagnose problems, and for related purposes. The Login.gov analytics dashboard generates reports and logs on population activity such as the percentage of successful sign-ins or the total number of users and can be accessed by all privileged Login.gov users. These reports do not include any metadata or PII. Login.gov provides agency partners with access to similar types of reports for their application user population. OCS AQS users may view the Login.gov website policy and PIA for additional information.

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

The OCS AQS follows the NIST 800-53 controls and DOI security and privacy control standards for user access based on least privilege to ensure that only authorized individuals have system access and can perform tasks as defined by their assigned roles.

The OCS AQS is not intended to monitor individuals. However, the system has the functionality to audit user activities. The OCS AQS login screen warns users that any unauthorized use of or access to the OCS AQS may subject violators to criminal prosecution and penalties. 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.

All DOI, BSEE, and BOEM employees and other users with access to Federal information or information systems (i.e., detailees, contractors, grantees, volunteers, interns, and other affiliates) must complete IMT Awareness Training and the Information Systems Security Rules of Behavior Acknowledgment before acquiring network and/or system access and annually thereafter. Individuals with significant privacy and security responsibilities must also complete role-based training. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, and criminal, civil, and administrative penalties.

The Login.gov PIA describes the controls used to prevent unauthorized monitoring of the system, including but not limited to least-privileged access, mandatory training, background check investigations for privileged users, and audit logs.

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: The system inherits controls from Login.gov for authentication.

(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: The system inherits controls from Login.gov for authentication.

(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: The system inherits controls from Login.gov for authentication.

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 Atmospheric Scientist within the Branch of Physical/Chemical Sciences is the OCS AQS Information System Owner. The OCS AQS Information System Owner and Information System Security Officer are responsible for ensuring that DOI, BSEE, and BOEM employees and contractors implement adequate safeguards to protect individual privacy and agency data in compliance with applicable Federal laws and policies. The BOEM Associate Privacy Officer (APO) will coordinate with the OCS AQS Information System Owner and other appropriate officials to address any reported privacy-related complaints or concerns in a timely manner.

GSA is responsible for the management of Login.gov and for protecting individual privacy for the information collected, maintained, used, and transmitted by GSA for identity verification and authentication purposes, and for meeting the requirements of the Privacy Act.

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 overseeing and managing the system's security and privacy controls and ensuring the proper management of data. The OCS AQS Information System Owner and the OCS AQS Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized disclosure, or unauthorized access to data is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures, as well as for coordinating with the BOEM APO to mitigate any impacts to individual privacy in accordance with the DOI Privacy Breach Response Plan and the BSEE Incident Response Procedures. The OCS AQS Information System Owner and the OCS AQS Information System Security Officer are also required to report any breaches or compromise of authentication information provided by Login.gov.

GSA is responsible for Login.gov and the management and security of PII data submitted by individuals for identity verification and authentication purposes and for reporting any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data that may impact DOI upon discovery in accordance with Federal policy and established procedures.