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: Technical Information Management System (TIMS)
Bureau/Office: Bureau of Safety and Environmental Enforcement (BSEE)/Technical Services Division
Date: March 26, 2021
Point of Contact:
Name: Rowena Dufford
Title: BSEE Associate Privacy Officer
Email: privacy@bsee.gov
Phone: 703-787-1257
Address: 45600 Woodland Road, Sterling, VA 20166

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 Technical Information Management System (TIMS) is a critical information system that automates many of the business and regulatory functions supporting the Bureau of Ocean Energy Management (BOEM) and the Bureau of Safety and Environmental Enforcement (BSEE); it is maintained and operated by the BSEE Office of Administration.

BOEM is responsible for managing development of the nation's offshore resources in an environmentally and economically responsible way. BOEM functions include Leasing, Plan Administration, Environmental Studies, National Environmental Policy Act Analysis, Resource Evaluation, and

Economic Analysis. BSEE is responsible for enforcing safety and environmental regulations. BSEE functions include all field operations including Permitting and Research, Inspections, Offshore Regulatory Programs, Oil Spill Response, and the newly formed Training and Environmental Compliance functions.

TIMS supports the central mission of the two bureaus and enables the regional (Alaska, Denver, Gulf of Mexico, and Pacific) and headquarters (Sterling, VA) staff to share and combine data; create and print maps; capture efficiencies through standardization of processes, forms, reports, and electronic submissions of data; and reduce the costs associated with setting up and maintaining duplicate databases, information storage and retrieval systems.

Data in TIMS is overwhelmingly business and regulatory information. This assessment, however, addresses the comparatively small amount of information related to individuals, while the majority of which is related to user access credentials and information related to an individual's business capacity (e.g., business contact information), some information may be personal contact information related to subscriptions for public information releases.

C. What is the legal authority?

The Outer Continental Shelf Lands Act (OCSLA), 43 U.S.C. 1331 et. seq., established federal jurisdiction over the submerged lands of the continental shelf seaward of state boundaries and charges the Secretary of the Interior with the responsibility for administering minerals exploration and development in the OCSLA, as well as formulating regulations to meet the provisions of the OCSLA.

Legal authorities that permit BOEM and BSEE to collect the information of stakeholders interested in receiving information from the bureaus include the following: 44 U.S.C. 3501, Paperwork Reduction Act of April 7, 2010; 5 U.S.C 301, Departmental Regulations; The President's January 21, 2009 memorandum on Transparency and Open Government; Presidential Memorandum on Building a 21st Century Digital Government, May 23, 2012; OMB Memorandum M-10-06, Open Government Directive, December 8, 2009; and OMB Memorandum on Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act.

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:

The UII Code for TIM is 010-000000226 00-22-01-03-01-00. The BSEE System Security and Privacy Plan (SSP) for TIMS is available in CSAM.

☐ 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	Describe
TIMSWeb	TIMSWeb is the new user interface which serves as the access point to TIMS.	Yes	Database user ID and password. Business contact: Name, Address, Phone Number, Email, and Transaction Number. Witness contact information in accident investigations: Name, Address and Phone Number.
TIMS Legacy	TIMS Legacy is the user interface which serves as the access point to legacy forms and reports.	Yes	Witness contact information in accident investigations: Name, Address, and Phone Number.
National Consolidated Information System (NCIS)	NCIS contains TIMS data and the Organizational Development and Support (ODS) Tracking Application.	Yes	NCIS: Database user ID and password. Business contact: Name, Address, Phone Number, and Email. ODS Tracking Application: Database user ID and password. BOEM personnel-related information regarding Gulf Region positions, such as position titles and their associated pay plan, occupational series grade, and the position incumbent's name (if applicable); and the status of personnel-related actions (e.g., staffing, details, promotions, and retirements).
Electronic Document Management System (EDMS)	EDMS stores and maintains documents.	Yes	Business contact: Name, Address, Phone Number, and Email.

Subsystem Name	Purpose	Contains PII	Describe
Geological Interpretation Tools (GIT)	GIT is a set of applications used to analyze and interpret geophysical and geological information to support the pre-lease and post-lease sale programs.	Yes	User ID and password. Business contact: Name, Address, Phone Number, and Email.
BOEM/BSEE Data Center	The Data Center allows for the purchase and download of publicly releasable data and documents. It also allows individuals to sign up for newsletters along with other types of program notices and updates.	Yes	User ID and password. Personal/business contact: Name, Address, Phone Number, Email, Transaction Number and History.
National Response Center (NRC) Reports	This system is designed to upload data, nightly, from the NRC, which is run by the US Coast Guard. It allows BSEE to document analytical information on incidents contained in the reports. This is designed for BSEE/BOEM internal use only.	Yes	Contact information to include name, phone number and email. If applicable, business name. It may also include information about the responsible party for the incident.

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

☒ Yes: TIMS does not require publication of a system of records under the Privacy Act of 1974. However, DOI login credentials to access TIMS is covered by DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), and purchase transactions externally made by individuals on Pay.gov for publicly available documents in TIMS are covered by DOI-86, Accounts Receivable: FBMS. The subscriptions services for the BOEM/BSEE Data Center are covered under DOI-08, DOI Social Networks.

☐ No

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

☒ Yes:

- Assignment of Federal OCS Pipeline Right-of-Way Grant-Reporting Instructions (1014-0016) (BSEE, expires 10/31/2021)
- Application for Permit to Drill (1014-0025) (BSEE, expires 6/30/2023)
- 30 CFR Part 250, Subpart G, Well Operations and Equipment (1014-0028) (BSEE, expires

1/31/2023)
- End of Operations Report (1014-0018) (BSEE, expires 2/29/2024)
- Performance Measures Data (1014-0017) (BSEE, expires 12/31/2021)
- Hurricane and Tropical Storm Evacuation and Production Curtailment Statistics - Gulf of Mexico OCS Region (1014-0022) (BSEE, expires 2/29/2024)
- Semiannual Well Test Report (1014-0019) (BSEE, expires 1/31/2023)
- 30 CFR 250, Subpart H, Oil and Gas Production Safety Systems (1014-0003) (BSEE, expires 1/31/2022)
- 30 CFR 254, Oil-Spill Response Requirements for Facilities Located Seaward of the Coast Line (1014-0007) (BSEE, expires 12/31/2021)

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Email Address
☒ Employment Information
☒ Mailing/Home Address
☒ Other: Personal email, mailing and home addresses are for Data Center use only. In giving contact information, individuals may include personal cell and home phone numbers.

Internet Protocol (IP) addressees are collected for internal network users only.

Other categories of PII include the following: Business contact information (e.g., email, phone number, and mailing address) for individuals in their business capacity, typically for energy companies; and transaction numbers of Data Center purchases. Actual financial information related to purchases are made through Pay.gov and are not maintained in TIMS. The Bureau of the Fiscal Service, U.S. Department of the Treasury, manages Pay.gov and has made the system PIA available on its website.

The ODS Tracking application contains the names of current and onboarding BOEM employees and generally non-sensitive information associated with their position.

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: Oil and gas lessees/operators can submit the names of personnel who should have access (e.g., username and password) to their own company data in TIMS. It also contains information on individuals

performing duties on behalf of these companies (i.e., non-sensitive, business-related contact information).

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: Internet-based TIMS Web forms and company-supplied media.

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

Information about individuals is used to validate the personnel of companies who do business on the OCS; to provide a point of contact to answer questions or concerns about the company's operations or submitted information; and to issues user credentials to access and submit company data in TIMS.

Witness contact information is used to support accident investigations, and may include name, address and phone number to contact witnesses for additional information regarding an incident or accident that occurs in the OCS.

The BOEM/BSEE Data Center collects PII from individuals (i.e., email and mailing addresses which may be personal or business-related) for registration purposes in order to process free subscriptions to recurring public information releases, as well as purchase transactions of releasable data and documents. Actual financial information related to purchases, such as bank account or credit card information, is collected through Pay.gov and not maintained in TIMS.

The ODS Tracking application provides enhanced human capital management capabilities to ensure that BOEM's Gulf Region—which employs the majority of the bureau's personnel—is equipped to support the bureau's mission and effectively liaison with BSEE, which provides Human Resources services to BOEM.

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

☒ Within the Bureau/Office: Administrators for the TIMS create user access credentials. Authorized BOEM and BSEE personnel may use the data to contact company officials. Authorized BOEM and BSEE personnel in the Bureau Public Affairs Offices use the data to transmit requested documents to complete Data Center purchase transactions and fulfill subscription requests. Bureau Public Affairs Officials may receive subscriber data exports to help manage subscription services. ODS Tracking application users may share organizational charts and human capital management reports with BOEM managers to ensure that BOEM's Gulf Region, which employs the majority of the bureau's personnel, is equipped to support the bureau's mission and effectively liaison with the BSEE Human Resources Office.

☒ Other Bureaus/Offices: TIMS provides measurement locations and metering points; well status; lease status; and other non-PII data to the Office of Natural Resources Revenue (ONRR) for the collection of royalties from oil and gas lease owners and operators. ONRR has read-only access to company-related data on leases and production to ensure the proper collection of lease fees and royalties; this includes access to business contact information.

☒ Other Federal Agencies: Certain regulations and agreements require BOEM/BSEE to share public information (i.e., scrubbed of sensitive proprietary data and/or other non-public business information) on permits, Exploration Plans, and Development Plans with other Federal agencies, such as the National Marine Fisheries Service, Environmental Protection Agency, and the U.S. Coast Guard; these documents may contain business contact information.

The Data Center redirects individuals who wish to purchase publicly releasable data to Pay.gov (a secure service provided by the Department of Treasury) in order to process payment. When redirected, information the purchaser inputs their name and address into the Data Center Order Form fields automatically prepopulates the form in Pay.gov where the purchaser then provides their payment information. Purchasers are able to edit their name and mailing address (home or business) on Pay.gov. Financial information is not routed back to TIMS or the Data Center, it is processed through Pay.gov and the Financial and Business Management System (FBMS). Only a transaction confirmation is returned to the Data Center. Once the successful transaction is completed in Pay.gov, purchasers are returned to the Data Center where the completed transaction is stored; the order confirmation/receipt with the requested information is sent to both the purchaser and the Office of Public Affairs for BOEM or BSEE, as applicable, which sends the requested public information and completes the transaction.

In addition, information may be shared under the routine uses described in Privacy Act systems of records notices DOI-08, DOI Social Networks, DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), and DOI-86, Accounts Receivable: FBMS, which may be viewed on the DOI SORN Web page at https://www.doi.gov/privacy/sorn.

☒ Tribal, State or Local Agencies: Certain regulations and agreements require BOEM/BSEE to share public information on permits, Exploration Plans, and Development Plans with agencies, such as State Coastal Zone Management and Governors' offices as outlined in agreements with each state in compliance with the Coastal Zone Management Act of 1972. This information may contain business contact information.

In addition, information may be shared under the routine uses described in Privacy Act systems of records notices DOI-08, DOI Social Networks, DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), and DOI-86, Accounts Receivable: FBMS.

☒ Contractor: Contractors who perform system administration may have access to PII stored in TIMS during the course of their duties.

☐ Other Third Party Sources

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

☒ Yes: Individuals seeking to purchase publicly releasable data can limit the information they provide to the Data Center and/or Pay.gov; however, in doing so BOEM/BSEE may not be able to fulfill their request.

In order to conduct business on the OCS, 30 C.F.R. 250 requires companies to provide official points of contact. However, the choice to conduct business on the OCS is voluntary.

☐ No

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

☒ Privacy Act Statement:

A Privacy Act Statement is provided on the Data Center Email Subscription page:
BOEM and BSEE are requesting your contact information in order to send you information via email subscription service. You may sign up by selecting the topics that interest you and entering your contact information in the contact box below. You will be required to verify your e-mail address before receiving list notices.

The collection of your contact information for this form is authorized under OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies and 5 U.S.C 301, Departmental Regulations. BOEM and BSEE will use your information to manage your subscription and will not share your information with third parties for promotional purposes. BOEM and BSEE do not routinely share subscriber information with external agencies unless required by law, or as authorized under the Privacy Act or the routine uses in DOI-08, DOI Social Networks, 76 FR 44033 (July 22, 2011), which may be viewed at https://www.govinfo.gov/content/pkg/FR-2011-07-22/html/2011-18508.htm. Providing this information is voluntary, but it is necessary to participate in available subscription services. You may unsubscribe at any time and may access the information directly on BOEM.gov or BSEE.gov.

A Privacy Act Statement is provided on the registration page where individuals create accounts or complete forms on Pay.gov to purchase products:
Authority: The information requested is authorized by 30 CFR 250.197, 30 CFR 550.197, and 30 CFR 551.14.
Purpose: To allow access to and purchase of publicly releasable data and documents.
Routine Uses: The information on this form may be shared outside the DOI as follows: to the Department of Treasury to process payment information. More information about the routine uses can be found in system of records notice, Accounts Receivable: FBMS, DOI-86.
Disclosure: Providing the requested information is voluntary but if not provided we will not be able to process your request.

☒ Privacy Notice: Privacy Notice is provided through the publication of this PIA; the DOI-08, DOI Social Networks SORN; the DOI-47, Logical Security Files SORN; the DOI-86, Accounts Receivable: FBMS SORN; the FBMS PIA; and the Department of the Treasury, Bureau of Fiscal Service .013-Collections Records SORN.

☒ Other:
Related information collections contain all requisite notices. All TIMS modules contain a Privacy Notice:

TIMSWeb Privacy Notice: 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, 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. 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.

☐ 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/BSEE typically do not use personal identifiers to retrieve records in TIMS. Incident records are retrieved by lessee or operator name.

Data Center administrators and customers (i.e., individuals who have purchased releasable data) can retrieve purchase transaction information by the purchaser's name or transaction number.

I. Will reports be produced on individuals?

☒ Yes: Purchase history reports from the Data Center are available to the purchaser and administrator. For example, the administrator may request reports to verify shipping address and determine who ordered data that BOEM or BSEE incorrectly released.

☐ No

Section 3. Attributes of System Data

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

Individuals conducting Data Center purchase transactions are expected to submit accurate information in order for BOEM/BSEE to complete their request. In the event individuals have submitted inaccurate information, they may update their user information in the Data Center, or contact BOEM/BSEE to correct any errors.

Individuals subscribing to recurring publicly releasable information are expected to submit accurate information in order for BOEM/BSEE to complete their request. Individuals are able to update their contact information if it changes.

Oil and gas lessees/operators are responsible for the accuracy of the information they provide in order to conduct business with BOEM/BSEE. Company representatives are required to include their names, email address, phone, and address in permit requests, plans, reports, and other documents they submit to BOEM/BSEE for consideration. BOEM/BSEE do not validate the business-related contact information and only use it to contact company representatives if BOEM/BSEE has approved their company's request or if additional information about the company's plan, permit, or report is needed. In cases where there is established business between BOEM/BSEE and a company, only specific individuals are authorized by the company to conduct business on its behalf. In those cases, BOEM/BSEE will validate the name and title of the submitter against the official company records in the TIMS database.

B. How will data be checked for completeness?

Individuals conducting Data Center purchase transactions are expected to submit complete information in order for BOEM/BSEE to complete their request. In the event individuals have submitted incomplete information, they may update their user information in the Data Center, or contact BOEM/BSEE to correct any omissions.

Individuals subscribing to recurring publicly releasable information are expected to complete required fields in order for BOEM/BSEE to complete their request. Individuals are able to update their contact information if it changes.

Companies that submit information to BOEM/BSEE are responsible for the completeness of the information they have provided. Incomplete data may result in their exclusion from consideration from conducting business with the bureaus.

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

Information entered by individuals conducting Data Center purchase transactions are a snapshot in time and the need for up-to-date information is only essential until BOEM/BSEE completes the transaction. Information from individuals subscribing to recurring publicly releasable information is a snapshot in time and subscribers are able to update their contact information if it changes. ODS staff are responsible for maintaining updated BOEM personnel-related information in the ODS Tracking application to provide real-time reports and ensure timely processing of personnel-related actions. Companies that submit information to BOEM/BSEE are responsible for the currency of information on file at BOEM/BSEE and are required to inform BOEM/BSEE if a company official's information changes.

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

The documents, plans, permits, and reports in TIMS have life-cycle and retention schedules. Data associated with those documents, plans, permits, and reports would follow the same retention schedule, unless specified as different. Energy-related records in this system are retained and disposed in

accordance with the applicable item numbers in the following National Archives and Records Administration (NARA), Department Records Schedules (DRS):

- N1-589-12-003 BOEM Analysis and Evaluation of Outer Continental Shelf (OCS) Resources
- N1-589-12-004 Energy and Mineral Leases (BOEM)
- N1-589-12-005 Records of Regulatory Oversight and Stewardship (BOEM)
- N1-473-12-003 Records of Analysis and Evaluation of Outer Continental Shelf (OCS) Resources (BSEE)
- N1-473-12-004 Records of Energy and Mineral Leases (BSEE)
- N1-473-12-005 Records of Regulatory Oversight and Stewardship (BSEE)

Retention periods for the schedules above vary from item to item and range from temporary to permanent. Also, records retention periods are also subject to litigation holds, court orders, and preservation notices issued by the Office of the Solicitor and may require the retention of these records past their cutoff date.

Data Center purchase transaction records are maintained under the DRS-1 Long Term Financial and Acquisition Records (DAA-0048-2013-0001-0011). These are financial/acquisition records that require additional retention, generally to conform to preservation standards in specific regulations, policies, or other legal/statutory requirements. These records may be more comprehensive and complete records, involve interaction with the public in a manner that necessitates longer protections, or support a financial obligation. Records covered under DAA-0048-2013-0001-0011 have a temporary disposition and will be destroyed 7 years after cut off as instructed in the agency/bureau records manual, or at end of fiscal year in which files are closed if no unique cut-off is specified.

ODS Tracking application records are maintained under the DRS-1 – Administrative schedule (DAA-0048-2013-0001, 1.2 Human Resources Management, A. [0004] Short-term Human Resources Records and D. [0009] Human Resources Records of Specific Temporary Value). Records covered under this schedule have a temporary disposition and will be destroyed 3 years after cut-off (item A) or when no longer needed (D).

System administration or Active Directory (AD) records are maintained under the DRS Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer term justification of the bureaus/offices activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cut-off. Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version upon termination of the system and destroyed three 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?

Records are disposed of in accordance with the applicable record schedule and Departmental policy. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing

for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

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

TIMS automates many of the business and regulatory functions supporting BOEM and BSEE. The TIMS supports the central mission of the two bureaus and enables the regional (Alaska, Denver, Gulf of Mexico, and Pacific) and headquarters (Sterling, VA) staff to share and combine data; create and print maps; capture efficiencies through standardization of processes, forms, reports, and electronic submissions of data; and reduce the costs associated with setting up and maintaining duplicate databases, information storage and retrieval systems.

Information in TIMS subsystems related to individuals–excluding some information in the Data Center and the NCIS database–is of a business nature (e.g., the name of an individual authorized to perform business transactions on behalf of a company, company name and business mailing address, phone number and email address) and is collected via an electronic form through a secure file transfer. This provides oil and gas industry users with the ability to submit online requests for company, qualification, merger and bonding information for review and approval. The Data Center, accessed by both individuals and representatives of companies, provides publicly releasable data and documents for download and/or purchase. The ODS Tracking application contains limited BOEM personnel-related information to facilitate human capital management activities in the Gulf Region.

Data Center users must register with their name, contact information and company affiliation (if applicable) in order to conduct transactions. Data Center registrants can check their order status, purchase history, and manage their accounts. BOEM and BSEE collect any applicable Data Center transaction fees via Pay.gov, a secure Department of the Treasury service, for the primary purpose of conducting secure financial transactions with federal agencies. There is a minimal risk to privacy due to the limited PII maintained in the Data Center database for purchase transactions, which includes names, mailing or email addresses, and whether payment has been received; actual financial or payment account information is not processed or maintained in TIMS or the Data Center. Payment information is processed through the FBMS, and privacy risks associated with the use of FBMS were assessed in the FBMS PIA, which may be viewed on the DOI PIA Web page at https://www.doi.gov/privacy/pia.

There are is minimal risks to the privacy of individuals associated with the handling, processing, or storing of their PII in TIMS subsystems. BOEM/BSEE have taken several steps to safeguard the integrity of TIMS, including but not limited to authentication, monitoring, auditing and encryption. Security measures have been integrated into the design, implementation and day-to-day practices of the entire operating environment as part of the bureaus' continuing commitment to risk management.. Privacy risks are mitigated by a combination of administrative, physical and technical controls. Access to TIMS is role-based. TIMS follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. All TIMS users (internal and external) must be authorized and approved to access TIMS and annually sign a DOI Rules of Behavior form. Access to output capability (i.e., forms and reports) is also role-based. Industry user access is controlled by company ID, user ID and password. Users representing BOEM-qualified companies can view and modify their company's data only. There is little risk of one company accessing data from another, as company designation and user roles prevent cross-sharing of information.

There is a risk to subscriber data used by the bureaus for unauthorized purposes, including, but not limited to, transferring info to third-party platforms without subscriber consent. This risk is mitigated by ensuring that individuals with access to subscriber data complete annual privacy awareness and role-based privacy training, as well as informing subscribers about changes before their implementation so they can opt out.

There are mandatory requirements for employees and contractors of BOEM and BSEE to complete information security, privacy, and records management training before getting access to any BOEM or BSEE system, including but not limited to TIMS. Internal TIMS access is controlled by information from Active Directory that is shared with TIMS for the purpose of authenticating users and managing access. Users no longer requiring TIMS access (e.g., departure of a designated company representative or separation of a BOEM or BSEE employee from service) are required to submit a new form to request access suspension. Other federal agencies do not have direct access to the system. However, data may be shared with other federal agencies as necessary to meet legal or mission requirements in the course of conducting official business. Authorized sharing with external agencies will be made pursuant to bureau mission authorities and applicable system of records notices for each use.

Federal Government information is managed and safeguarded by following National Institute of Standards and Technology (NIST), the Federal Information Security Modernization Act of 2014 (FISMA), and DOI security and privacy policies. TIMS is hosted in a secure DOI data center protected by physical and network security controls. TIMS has a Moderate system security categorization in accordance with NIST standards, Federal Information Processing Standards 199, and FISMA. The TIMS SSP describes appropriate security controls implemented to safeguard TIMS information collection, use, retention, processing, disclosure, destruction, transmittal, storage and audit logging. All access is controlled by authentication methods to validate the authorized user. Note: A risk-based decision was made by the Authorizing Official not to encrypt tape backups due to high cost and key management complexity. Currently tapes are containerized, secured and stored in a controlled offsite facility. However, due to new OMB requirements, tape backup media must be encrypted. The bureau will explore the feasibility of backup tape encryption.

The TIMS login pages greets all users with a Privacy Notice banner on the TIMS login page which informs users that they have no explicit or implicit expectation of privacy. Audit trails of activity are maintained to reconstruct security relevant events. The audit trail will include the identity of each user accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security.

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 collected is relevant to perform functions of the TIMS subsystem which support BOEM and BSEE missions. For the Data Center, the data is relevant and necessary to complete purchases and fulfill requests for program notifications.

☐ 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?

No new data about individuals is created in TIMS.

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

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

Business Users: Must have a valid user ID and password and are limited by roles. Users must submit an access request form that is vetted by validation of name and title of the submitter against the official

company records on file. Users are restricted to viewing their own company's data.
Data Center Users: Must have a valid user ID and password to purchase data. Users are restricted to viewing their own purchase history data.
Internal Users: Must be authenticated by Personal Identity Verification (PIV) card and Personal Identification Number (PIN) and are limited by roles.
Application Administrators: Must be authenticated by username and password; level of access is determined by role.
System Administrators: Must be authenticated by PIV card and PIN; level of access is determined by role.
Subscribers: Individual subscribers can only request changes to their own subscription preferences.

TIMS uses the principle of least privilege access for authorized users to perform duties as defined by business rules. Federal Government information is managed and safeguarded by following FISMA, NIST guidelines, and DOI security and privacy policies.

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. Personnel, physical and logical security contract clauses were also 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. For all users, in accordance with NIST 800-53 controls, audits logs are maintained on user activity in TIMS. This includes valid and invalid logins, purchase transactions, IP addresses, etc.

For the backend database, user activities are logged (add, edit, delete).

☐ 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. Information collected is used to monitor user access (username) and activity (logins, record changes, deletions, additions, date and time-stamp) for auditing purposes.

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

TIMS uses the principle of least privilege access for authorized users to perform duties as defined by business rules. Only administrators can access the logs. This is a technical control of the data storage system. For example, only database administrators can view database logs.

All administrators must complete Role-Based Security training, Role-Based Privacy training and sign a Rules of Behavior form acknowledging their elevated access responsibilities.

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 Chief, Technical Services Division, is the TIMS System Owner. The System Owner oversees and manages the protection of agency information processed and stored on TIMS. The TIMS System Owner and Information System Security Officer, in collaboration with the TIMS Data Stewardship Officer, the bureaus' Senior Management Teams and Associate Privacy Officers, are responsible for ensuring adequate safeguards are implemented to protect individual privacy and addressing complaints in compliance with Federal laws and policies for the data managed, used, and stored on TIMS.

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 TIMS 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 TIMS System Owner and ISSO are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC, the DOI incident reporting portal, in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in consultation with the bureaus' Associate Privacy Officers.

The BSEE Incident Response Team handles incidents for BOEM/BSEE in accordance with BSEE incident response policy and the DOI Privacy Breach Response Plan, which provides guidance on breach response, the process for timely notification to individuals, and other remedial actions.