U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior (DOI) 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: BOEM Auction System (BAS)
Bureau/Office: Bureau of Ocean Energy Management (BOEM)
Date: February 8, 2024
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 has the authority to issue leases, easements, and rights-of-way on the Outer Continental Shelf (OCS) using a competitive or a non-competitive process. When BOEM uses a competitive process, it awards offshore lease areas through a simultaneous ascending clock auction format using a configurable web-based application in a cloud-hosted environment. The number and configuration of lease areas to be offered is determined by BOEM.

For each lease sale, BOEM publishes a Proposed Sale Notice (PSN) in the *Federal Register*, followed by a 60-day comment period. The PSN includes a statement of the proposed auction format and related parameters and procedures. During the PSN comment period, BOEM and the auction services provider host a public auction seminar to discuss the auction process and format.

After a period of comment review determined by BOEM, BOEM publishes a Final Sale Notice (FSN) in the *Federal Register*, followed by a 30-day waiting period before an auction may take place. The FSN provides the list of eligible bidders and detailed auction rules, parameters, and procedures. It also reflects any changes from the PSN in response to public comments received or further internal review by BOEM.

Bidders at BOEM's offshore auctions are required to be legally, technically, and financially qualified in advance of the auction, with the end of the PSN comment period being the deadline for submitting qualifications for the auction. Bidders submit their qualification applications directly to BOEM. A list of qualified bidders is transmitted by BOEM to the auction services provider approximately five days after the FSN is published in the *Federal Register.*

The auction services provider configures the auction system based on the information provided by BOEM and conducts the lease sale auction. Following the conclusion of the auction, the auction services provider closes the auction and provides the final data and reporting services to BOEM. Winning bidders are notified in writing by BOEM of bid acceptance following the auction.

BOEM will use the BOEM Auction System (BAS) to conduct the monetary stage of offshore energy lease sales. BAS, which replaces the Auction of Wind Lease System (AOWLS), is the cloud-based lease auction application service that the bureau will use to conduct and support auction operations for individual offshore lease sales. BOEM will use Login.gov to authenticate users to provide access to BAS. Login.gov is a platform owned and operated by the U.S. General Services Administration (GSA) through which members of the public can sign in and access information and services from participating Federal agencies.

C. What is the legal authority?

The Outer Continental Shelf Lands Act (OCSLA) at subsection 8(p) (43 U.S.C. 1337(p)) authorizes the Secretary of the Interior to issue leases, easements, or rights-of way on the OCS for activities that produce or support the production, transportation, or transmission of energy from sources other than oil and gas, including renewable energy. The Secretary delegated this authority to BOEM. BOEM has issued regulations for OCS renewable energy activities at 30 CFR Part 585, including sections 211 and 216.

The Login.gov service is operated by GSA under the authorities and guidance found in the E-Government Act of 2002, 6 U.S.C 1523 (b)(1)(A)-(E), 40 U.S.C 501, and Office of Management and Budget (OMB) Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management.

Pay.gov is a program operated by the Bureau of the Fiscal Service (BFS) in the U.S. Department of the Treasury (Treasury) under the following authorities: 5 U.S.C 301, 31 U.S.C 321, 31 U.S.C Chapter 33, and 31 U.S.C 3720.

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: The UII Code is 010-000001875. A System Security and Privacy Plan is under development for BAS.

☐ 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
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: BAS does not create a system of records. However, GSA and Treasury have published SORNs that cover Login.gov and Pay.gov records. GSA maintains records on individuals who use Login.gov and has published a SORN for the system, GSA/TTS-1 (Login.gov), 82 FR 6552 (January 19, 2017); modification published 82 FR 37451 (August 10, 2017) and 87 FR 70819 (November 21, 2022). The SORN is available for review on the GSA SORNs web page. Treasury maintains records on individuals who electronically authorize payments to the Federal Government through the use of communication networks, including but not limited to Pay.gov, and has published FS. 013 – Collections Records – 85 FR 11776 (February 27, 2020). The SORN is available for review on the BFS SORNs web page.

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

☐ Yes

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Other: BAS does not collect, process, or maintain the sensitive personally identifiable information (PII) of individuals. BOEM collects limited non-sensitive, business-related contact information from the representatives of qualified bidders (i.e., companies) to authorize their participation in a lease sale. Authorized company representatives will receive access to BAS to participate in the auction for which their company has qualified to bid by meeting all legal, technical, and financial participation requirements.

Each bidder must submit a Bidder's Financial Form (BFF) to BOEM to participate in the auction. BOEM must receive each bidder's BFF no later than the date listed in the FSN. Through the BFF, BOEM collects the name, work phone number, company mailing address, email address, and fax number of a company's 1) principal point of contact, 2) designated Electronic Funds Transfer and Pay.gov payment contacts, and 3) up to three individuals nominated to be authorized to bid on behalf of the company. On the BFF, eligible bidders also must list any other person with whom they are affiliated. For the purpose of identifying affiliated entities, a bidding entity is any individual, firm, corporation, association, partnership, consortium, or joint venture (when established as a separate entity) that is participating in the same auction. Affiliated entities are not permitted to compete against each other in the auction.

Each qualified bidder must submit a bid deposit no later than the date listed in the FSN. Once BOEM has processed a bidder's BFF, the bidder's designated Pay.gov contact can follow established processes to submit a bid deposit through Pay.gov. BOEM does not maintain information pertaining to financial transactions completed on Pay.gov in BAS.

BOEM personnel and company representatives authorized to participate in an auction must use Login.gov to access BAS. The PII collected and used by GSA for authentication through Login.gov is maintained by GSA. GSA will share limited information (i.e., user email address and agency-specific universal unique identifier (UUID)) with BOEM to authenticate access to BAS. BOEM will not use Login.gov for identity verification, which requires individuals to provide sensitive PII (e.g., Social Security number, date of birth, and home address) to GSA for assurance that the same individual who created the Login.gov account is accessing a partner agency's service or information.

Login.gov requires individuals to create a user account for authentication by providing a valid email address and creating a password. Login.gov also requires users to set up multi-factor authentication (MFA) using one or more authentication methods such as face or touch unlock, a security key, an authentication application (app), Federal government employee or military identification, a text or voice message, or backup codes. BOEM personnel will use Login.gov to access BAS with their personal identification verification (PIV) card setup as a multi-factor authentication method. PIV cards are only used as an additional factor beyond email and password and cannot be used by themselves to sign into a Login.gov account. Authorized company representatives must purchase a FIDO compliant security key for use as the phishing-resistant MFA method.

Once a user creates a Login.gov account, that user's account information is assigned a master UUID to identify the user in Login.gov. This master UUID is only used within the Login.gov system. The user is assigned an additional agency-specific UUID for each agency the user accesses. The user's agency UUID and the minimum set of user account information that a partner agency identifies as needed to allow access to its services or information is provided only after the user consents to send that information. BOEM will identify BAS users by the email address they used to create their Login.gov account.

Authorized company representatives will be directed to an Auction Helpdesk Verification pass-thru screen the first time they have logged into BAS using Login.gov. The pass-thru screen will contain a quick response (QR) code for an authenticator app that authorized company representatives can scan using their phone's camera. Users may utilize any standard authenticator app. Authorized company representatives who need to contact the Auction Helpdesk for assistance must provide the 6-digit verification code generated by their authenticator app to verify their identity. The Auction Helpdesk can access the user's name, phone number, and email address for the purpose of providing requested support after a user has entered their verification code. Auction Helpdesk actions will be reflected in the system audit log and screenshots. Authorized company representatives may review the authenticator app's privacy policy to understand what data the service may collect from users and how the service will use the data. The authenticator app is installed on the user's smartphone and does not directly share information with BOEM. Auction Helpdesk Verification can be performed at any time by navigating to Auction Helpdesk Verification setup from the user menu in the sidebar.

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: Bidding in an auction is restricted to authorized company representatives who have been granted access to BAS. Companies are responsible for providing all information required

to participate in a BOEM auction in accordance with published procedures. On the BFF, eligible bidders must also list any persons with whom they are affiliated.

Login.gov gathers PII directly from individuals during account creation and when a user is modifying their Login.gov account information. Login.gov users must opt in to share any information with each partner agency. BAS users provide Login.gov with consent to share their email address and agency-specific UUID with BOEM for authentication purposes.

BOEM personnel will use Login.gov to access BAS with their PIV card as a multi-factor authentication method. BOEM collects information from individuals during the onboarding process to issue PIV cards.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Website
☐ Fax
☒ Telephone Interview: Verified BAS users can make use of telephonic bidding support if needed.
☒ Information Shared Between Systems: GSA collects information directly from individuals who create a Login.gov user account. Login.gov will share a user's email address and agency-specific UUID with BOEM to authenticate the user's access to BAS. BOEM personnel will use Login.gov to access BAS with their PIV card setup as a multi-factor authentication method. Authorized company representatives will use Login.gov to access BAS using a FIDO compliant security key as the authentication method.

☒ Other: Companies submit a qualification package to BOEM for each lease sale in which they would like to participate in accordance with published procedures. Each company must also submit a BFF to BOEM no later than the date listed in the FSN to participate in the auction. A company that is eligible to participate in the auction would identify on its BFF up to three individuals who would be authorized to bid on behalf of the company, as well as the designated Pay.gov contact and affiliated entities (if applicable).

Individuals authorized to bid in an auction on behalf of a company access BAS through authentication provided by Login.gov. Bid deposit payments are processed on Pay.gov. BOEM does not maintain information pertaining to bid deposit payments in BAS.

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

BOEM is responsible for 1) approving the list of bidders (companies) that can bid in the auction and 2) sending the list of individuals authorized to bid on behalf of qualified bidders to the auction services provider to facilitate the company representatives' access to BAS for a specified lease sale.

All qualified bidders must submit a BFF to BOEM by the date listed in the FSN to participate in the auction. A company that is eligible to participate in the auction will identify on its BFF up to three individuals who are authorized to bid on behalf of the company. A bid deposit can only be submitted by the authorized individual designated on the company's BFF. Only individuals who have been properly set up and linked to a company in Pay.gov can access the bid deposit page and submit a bid deposit on behalf of a company. The Office of Natural Resources Revenue (ONRR) will set up an account for the individual on Pay.gov using the email address specified on the form. If the designated Pay.gov contact already has an active account under the email address provided in the BFF, ONRR will link that address to the company Pay.gov account shortly after receiving and processing the BFF. ONRR will provide payment instructions to all Pay.gov contacts of qualified bidders via email. After BOEM processes the bid deposits, the auction services provider will send the authorized individuals for each company BAS access instructions, the bidder manual for BAS, and any auction system technical supplement that may be issued.

Prior to using BAS, qualified bidders who have met the requirements and deadlines for auction participation are encouraged to take part in a live connectivity test and may also participate in a mock auction. BOEM provides qualified bidders with the details of the test (including the date, time, and requirements for participating) ahead of time. BOEM and contractor Auction Managers are online managing and monitoring the system during the test and are available to respond to any questions. Each user should successfully perform secure authentication to the system using their Login.gov credentials, as well as setup their authenticator app to ensure they can later make use of telephonic bidding support if needed. This test also serves to verify that the user's hardware and browser can connect to the BAS without issues. BOEM will provide final details of the mock auction in the FSN.

The respective BOEM regional director has the discretion to change any auction detail specified in the FSN, including the date and time, if the regional director deems events outside BOEM's control may interfere with a fair and proper lease sale. Such events may include, but are not limited to, natural disasters (e.g., earthquakes, hurricanes, floods, and blizzards), wars, riots, acts of terrorism, fire, strikes, civil disorder, U.S. Federal Government shutdowns, cyberattacks against relevant information systems, or other events of a similar nature. In case of such events, BOEM will notify all qualified bidders via email, phone, and BOEM's website.

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

☒ Within the Bureau/Office: Companies seeking authorization to bid in an auction must provide BOEM with all required information in advance of the lease sale in accordance with published procedures. Authorized individuals within BOEM who are facilitating the auction will have access to company information as well as the names and non-sensitive, business-related contact information of individuals named in the BFF who may be authorized to bid on behalf of the company via BAS.

Login.gov passes the email address and agency-specific UUID of a BAS user to the BOEM system when a user successfully signs into BAS using the authentication service.

Authorized BOEM personnel can access the downloaded and archived BAS audit log for a completed auction at any point in time to support any investigations.

☒ Other Bureaus/Offices: A bid deposit can only be submitted by the authorized individual designated on the company's BFF. Only individuals who have been properly set up and linked to a company in Pay.gov can access the bid deposit page and submit a bid deposit on behalf of a company. Once ONRR receives all lease sale BFFs from BOEM, it will work with Pay.gov to set up an account for the designated Pay.gov contacts using the email address specified on the form. If the designated Pay.gov contact already has an active account under the email address provided in the BFF, ONRR will link that address to the company Pay.gov account shortly after receiving and processing the BFF. For both new and existing bidders, ONRR will send Pay.gov payment instructions to the designated Pay.gov contacts listed on the lease sale BFFs. After BOEM processes the bid deposits, the auction services provider will send the authorized individuals for each company the bidder manual for BAS, instructions for accessing the system, and any auction system technical supplement that may be issued.

☒ Other Federal Agencies: Companies must submit their bid deposit through Pay.gov (operated by Treasury) for their authorized representative(s) to acquire access to BAS for the specified lease sale. ONRR, on behalf of BOEM, shares the business-related email addresses of designated Pay.gov contacts listed on BFFs with Pay.gov to facilitate their payment of the bid deposit for a specified lease sale. BOEM does not share BAS data with Pay.gov and does not maintain financial transaction information in BAS.

BOEM shares a summary of all bids received in an auction with the Department of Justice (DOJ) immediately following a lease sale. This information is used as part of an antitrust review conducted by DOJ pursuant to 43 U.S.C. 1337(c), prior to the execution of the lease. DOJ will have up to 30-calendar days to conduct an antitrust review of the auction. The DOJ review is acknowledged in the PSNs and FSNs published by BOEM for each planned auction.

In addition to the disclosures generally permitted under the Privacy Act of 1974, records and/or information or portions thereof maintained as part of the systems of records created by

Login.gov and Pay.gov may be disclosed outside of GSA and Treasury as routine uses to other Federal agencies.

☐ Tribal, State or Local Agencies

☒ Contractor: BOEM is responsible for 1) approving the list of bidders (companies) that can bid in the auction and 2) sending the list of individuals authorized to bid on behalf of approved bidders to the auction services provider. The approved company representatives receive BAS access and instructions from the auction services provider.

BAS has a robust audit log that captures all events undertaken by all users in the system. Auction Managers monitor the audit log for suspicious behavior. Approved individuals who are off-site (i.e., off-site System Administrator and technical support) are only permitted to access BAS when given permission to do so by the Lead Auction Manager.

☒ Other Third Party Sources: In addition to the disclosures generally permitted under the Privacy Act of 1974, records and/or information or portions thereof maintained as part of the systems of records created by Login.gov and Pay.gov may be disclosed outside of GSA and Treasury as routine uses to other third parties.

Login.gov may share Login.gov user information with contracted third-party organizations for identity verification and authentication purposes. BAS users may review the Login.gov PIA for details on how GSA may share PII data with these third-party entities.

Pay.gov transaction data that is necessary for fraud screening is sent to third party vendors. Access to this data is limited based on the need-to-know principle, any sensitive PII/data is encrypted both during transmission and at rest, and appropriate controls are in place to ensure that there is no impact to public privacy. The Pay.gov Privacy and Security Policy contains a full list of the parties to whom Treasury may disclose the information collected on Pay.gov. Authenticator apps are generally self-contained on a user's smartphone and do not share information with any third parties. Users may review the authenticator app's privacy policy for more information.

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

☒ Yes: Bidding in an auction is restricted to authorized company representatives who have access to BAS. Companies must complete a BFF for each lease sale in which they are eligible to participate. This form establishes a designated authorized company representative to submit a bid deposit on behalf of the company and identifies the individuals who will participate in the auction. Individuals who complete and sign a BFF on behalf of a company must be on file with BOEM in the Company Qualification Package and are responsible for ensuring the form is complete. If BOEM does not receive the company's completed BFF by the specified deadline or the company does not submit a bid deposit following BOEM's acceptance of its BFF, company representatives will likewise not be authorized to participate in the lease sale.

BAS users must authorize Login.gov to share their PII data with BOEM to allow the bureau to recognize the users and authenticate their access to the system.

New and existing bidders must use Pay.gov to submit a bid deposit. Only individuals who have been properly set up and linked to a company in Pay.gov can access the bid deposit page and submit a bid deposit on behalf of a company. After BOEM processes the bid deposits, the auction services provider will send the authorized individuals for each company the bidder manual for BAS, system access instructions, and any auction system technical supplement that may be issued.

Authorized company representatives may review the authenticator app privacy policy to understand what data the app may collect from users before consenting to the app's collection and use of the information. BOEM does not require the use of a specific authenticator app. A user's failure to provide a verification code to the Auction Helpdesk may delay receipt of assistance.

☐ No

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

☒ Privacy Act Statement: Before Login.gov shares any user PII with a partner agency, Login.gov gains explicit consent from the user. The user must enter their password to provide that consent. Login.gov provides links to its Privacy Act Statement on both the sign in and create account pages.

☒ Privacy Notice: BAS does not create a system of records. However, GSA and Treasury have published SORNs that cover Login.gov and Pay.gov records. GSA has published GSA/TTS-1 (Login.gov), 82 FR 6552 (January 19, 2017); modification published 82 FR 37451 (August 10, 2017) and 87 FR 70819 (November 21, 2022). The SORN is available for review on the GSA SORNs web page. Treasury has published FS. 013 – Collections Records – 85 FR 11776 (February 27, 2020). The SORN is available for review on the BFS SORNs web page.

GSA has also published a PIA for Login.gov. The PIA is available for review on the GSA PIA web page. Treasury's BFS provides notice to individuals through the posting of the PIA for Pay.gov on its PIA web page. BOEM also provides notice through the posting of this PIA on the BOEM PIA web page hosted by the DOI Privacy Office.

Login.gov provides links to its Privacy & Security page on both the sign in and create account pages. Pay.gov provides users with a link to its Privacy and Security Policy that individuals can review prior to providing and/or submitting information.

Authorized company representatives may review the authenticator app privacy policy to understand what data the service may collect from users and how the service will use the data.

☒ Other: BOEM provides notice through the PSN and FSN published in the *Federal Register*. Companies can also review the Qualification Guidelines and the BFF and contact BOEM if they have any questions. BOEM also provides notice on the private form made available to companies submitting a bid deposit on Pay.gov to participate in an auction.

BOEM will host a public seminar during the PSN's 60-day comment period to discuss the lease sale process and the auction format. The time and place of the seminar will be announced by BOEM and published on the BOEM website. No registration or RSVP is required to attend.

As part of the BFF, authorized individuals for companies must sign a certification statement that contains system rules of behavior for bidders; non-bidding users must sign a BAS Rules of Behavior form managed by the auction services provider.

BOEM branding is included throughout the sign in and create account processes to ensure the user knows that Login.gov is disclosing information to the bureau to facilitate user access to BAS. The BAS login screen also features the required system use notification banner that provides privacy and security notices to system users consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and states that:

- Users are accessing a U.S. Government system;
- System usage may be monitored, recorded, and subject to audit;
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
- Use of the system indicates consent to monitoring and recording.

The system use notification banner will remain on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system via the sign in with Login.gov button.

Prior to using the Login.gov service, individuals must read and acknowledge that they accept the Login.gov Rules of Use published by GSA. In the event that the Login.gov service changes its terms of service, users will be given the option to agree or to decline the updated terms of service the next time they login.

A warning banner is displayed on Pay.gov that informs users they are accessing a Treasury program, are subject to being monitored, and have no expectation of privacy during use of the system. Pay.gov also provides users with a link to accessibility statements and agreement notices that individuals can accept or decline prior to providing and/or submitting information. By signing in to Pay.gov to submit a bid deposit, individuals are agreeing to the Pay.gov Rules of Behavior.

☐ None

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

BAS assigns a unique internal ID associated with each user account as well as each qualified bidder. BOEM personnel, Auction Managers, and System Administrators retrieve data from the BAS using this unique ID or the company name of the qualified bidder.

I. Will reports be produced on individuals?

☒ Yes: BAS user accounts are monitored through audit logs that associate user accounts with user activities. BAS has a robust audit log that captures all transactions. Auction Managers monitor the audit log for suspicious behavior. BOEM will download and archive the audit log following an auction. Authorized BOEM personnel can access the downloaded and archived audit log for a completed auction at any point in time to support any investigations.

Login.gov may produce compliance/audit reports on individuals' actions in the system for investigatory and fraud mitigation purposes. BAS users may review the GSA Login.gov PIA for information on reporting functions within the system and how GSA generates, uses, and shares reports on individuals.

Pay.gov reports can be generated to identify activity surrounding transactions and processes performed by individuals. Pay.gov maintains an audit log of system users to ensure they do not violate the system and/or BFS Rules of Behavior. Pay.gov users may review the Pay.gov PIA for information on reporting functions within the system and how the agency generates, uses, and shares reports on individuals.

The authenticator app privacy policy describes the personal data the service processes, how the service processes it, and for what purposes.

☐ No

Section 3. Attributes of System Data

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

Representatives of companies seeking authorization to bid in an auction voluntarily provide company information and their non-sensitive, business-related contact information for each auction. The representatives authorized to bind the company are required to certify to the truth and accuracy of the statements and information they have provided in the BFF on behalf of the company in accordance with 18 U.S.C. 1001 (fraud and false statements).

Activities of all BAS users are logged. BOEM publishes full bid results, including round-by-round results of the entire sale and exit bids, on its website after a review of the results and announcement of the provisional winner.

BOEM will rely on GSA for authentication services. Authentication allows a partner agency to distinguish a user account based on an email address provided by the user and provides a partner agency minimal assurance that the same individual who created the Login.gov account is accessing that partner agency's service or information. Login.gov ensures the accuracy and completeness of the user's email address and multi-factor authentication method by requiring the user to confirm their email address and utilize an acceptable multi-factor authentication method. BAS users may review the GSA Login.gov PIA for information on how GSA will check their PII for accuracy.

ONRR will link a designated Pay.gov contact's account to the entity on whose behalf they are making a bid deposit and the current lease sale number. ONRR will also provide contacts with Pay.gov instructions. A company's Pay.gov contact is responsible for providing accurate information while submitting a bid deposit. Pay.gov users may review the Pay.gov PIA for information on how Treasury will verify data collected from sources other than agency records.

The Auction Helpdesk relies on authorized company representatives to verify their identity during auctions using an authenticator app.

B. How will data be checked for completeness?

The individual who completes and signs the BFF on behalf of a company must be on file with BOEM in the Company Qualification Package and is responsible for ensuring the form is complete and submitted in accordance with published BOEM procedures. Following a review of the required information and receipt of the bid deposit, BOEM will provide the auction services provider with the business-related contact information of company representatives authorized to bid in an auction.

Login.gov ensures the accuracy and completeness of the user's email address and multi-factor authentication method by requiring the user to confirm their email address and utilize an acceptable multi-factor authentication method. BAS users may review the GSA Login.gov PIA for information on how GSA will check their PII for completeness.

Pay.gov ensures that fields required to perform a function are filled out to ensure completeness of the transaction. Pay.gov users may review the Pay.gov PIA for information how Treasury will check their data for completeness.

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

Companies seeking authorization to bid in an auction must submit a BFF to BOEM to satisfy the requirements of each auction in accordance with published procedures. Company representatives who are authorized to bind the company are required to certify to the truth and accuracy of the statements and information they have provided in the BFF they submitted on behalf of their company.

Login.gov collects PII directly from individuals using their identity authentication service to access BAS. Individuals are responsible for providing accurate information to GSA. As part of user documentation and trainings provided to qualified bidders, users will be instructed to associate the email account they have provided to BOEM for use in BAS with their Login.gov account. This email account must match between the two systems in order for users to authenticate.

Designated company Pay.gov contacts are responsible for providing accurate information while submitting a bid deposit on Pay.gov. Pay.gov has built-in validation features. For example, validation occurs for payments to ensure that scheduled collection dates are not in the past and to eliminate the possibility of zero-dollar transactions.

The authenticator app generates a six-digit one-time password which users must enter in BAS to verify their identity to receive assistance from the Auction Helpdesk.

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

BOEM maintains lease bid and sale records in accordance with N1-589-12-4 (Item 4F). These records have a temporary disposition with a cutoff at the close of the fiscal year or when the activity is completed. BOEM retains these records either onsite or at an offsite storage facility and deletes/destroys them 25 years after the cutoff.

BAS usage records are covered under Departmental Records Schedule 1.4, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001-0013) and System Planning, Design, and Documentation (DAA-0048- 2013-0001-0014). 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 of upon termination of the system and destroyed three years after cut-off.

GSA is responsible for managing its Login.gov records in accordance with the Federal Records Act and approved records retention schedules. The Login.gov PIA contains additional information about GSA's retention of Login.gov records.

Treasury is responsible for managing its Pay.gov records in accordance with the Federal Records Act and approved records retention schedules. The Pay.gov PIA contains additional information about Treasury's retention of Pay.gov records.

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

The auction services provider creates BAS user accounts and encrypts and stores the qualified bidders list provided by BOEM in the auction archive for review in the event the auction is contested. BOEM will download the auction archive files and audit log and maintain the records in accordance with the applicable records schedule. After completion of an auction, all data specific to the auction is deleted from the server by the auction services provider.

Approved disposition methods include shredding or pulping for paper records and purging, degaussing, or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy.

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 will conduct the monetary stage of auctions of offshore energy leases through BAS. BAS is rated as a Federal Information Security Modernization Act of 2014 (FISMA) Moderate system based upon the type and sensitivity of data and requires the implementation of strict security and privacy controls to protect the confidentiality, integrity, and availability of the data contained in the system.

There is a minimal risk to individual privacy, as BAS does not collect, process, or maintain sensitive PII. BOEM collects the non-sensitive, business-related contact information of individuals authorized to represent companies seeking to conduct business with BOEM to 1) approve the list of bidders (companies) that can bid in the auction and 2) send the list of individuals authorized to bid on behalf of qualified bidders to the auction services provider to facilitate the company representatives' access to BAS for a specified lease sale. As part of user documentation and trainings provided to qualified bidders, users will be instructed to associate their email account they have provided to BOEM for use in BAS with their Login.gov account. This email account must match between the two systems in order for users to authenticate. The Auction Helpdesk can access the user's name, phone number, and email address for the purpose of providing requested support after a user has entered their authenticator app verification code on the Auction Helpdesk Verification pass-thru screen. BOEM will evaluate the potential privacy risks generated by any proposed changes to the categories of information collected from individuals (i.e., authorized company representatives) during any stage of the auction process prior to the bureau's implementation of those changes.

There is a risk that individuals may not receive adequate notice of the extent of BOEM's use of the information that the bureau collects to conduct auctions. Companies that BOEM has acknowledged as eligible bidders in a FSN published in the *Federal Register* are responsible for providing all information required to participate in an auction in accordance with published procedures. BOEM provides companies and their designated representatives who will interact with the bureau and its service providers with notice at various points throughout the auction

process. BOEM provides notice through the published PSN and FSN, Qualification Guidelines, and the BFF. BOEM will also host a public seminar during the PSN's 60-day comment period to discuss the lease sale process and the auction format. Authorized company representatives must review and sign a rules of behavior form before acquiring access to BAS. Before logging into BAS, users may review a system use notification banner that provides privacy and security notices to system users consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. BOEM also provides general notice through the publication of this PIA.

There is a risk that individuals may not receive adequate notice of the privacy practices of Treasury (Pay.gov), GSA (Login.gov), and the developer of the utilized authenticator app. Pay.gov users submit bid deposits using Pay.gov and are subject to the Pay.gov Rules of Behavior. Companies and their designated representatives may review the Pay.gov Privacy and Security Policy, agreement notices, the FS. 013 – Collections Records SORN, and the Pay.gov PIA before they use the service to submit the required bid deposit. BAS users access the system through authentication performed via Login.gov and are subject to the Login.gov Rules of Use. Login.gov provides links to its security practices and Privacy Act Statement on both the sign in and create account page for authentication and identity verified accounts. BOEM branding is also included throughout the sign in and create account processes to ensure that individuals are aware that GSA will disclose information to BOEM. BAS users may review the GSA Login.gov PIA and the GSA/TTS–1 (Login.gov) SORN for details on the collection, use, storage, or sharing of their PII by GSA. Authorized company representatives may review their authenticator app's privacy policy before using the service to verify their identity to receive assistance from the Auction Helpdesk to understand how the service will collect and use their information.

There are risks of unauthorized access to and/or misuse of BAS and the information collected by BOEM to conduct the auction process. BOEM and its auction service provider can mitigate these risks by implementing the applicable security and privacy policies, procedures, and training requirements to control and monitor access to the system and auction-related information. BOEM is responsible for 1) determining who has privileged access (e.g., Auction Managers and BOEM staff), 2) approving the list of bidders (companies) that can bid in the auction, and 3) sending the list of individuals authorized to bid on behalf of approved bidders to the auction services provider. BAS has various access controls in place to limit access to authorized users based on assigned roles. All users must complete a rules of behavior form before being granted system access through multi-factor login credentials (as part of the BFF, authorized individuals for companies must sign a certification statement that contains system rules of behavior for bidders; non-bidding users must sign a rules of behavior form managed by the auction services provider). Approved individuals who are off-site (i.e., off-site System Administrator and technical support) are only permitted to access BAS when given permission to do so by the Lead Auction Manager. Auction Managers must only use their designated read-only account, except when given permission from the Lead Auction Manager to use the read/write Auction Manager account. In between auctions, the system is not online and cannot collect or process data. After each auction, all bidders' system access is disabled.

All BAS users are informed through the system notification use banner that use of the system is monitored and unauthorized system use may result in civil or criminal penalties. BAS has a robust audit log that captures all transactions to protect system and data integrity. During an auction, the Auction Manager team monitors the BAS audit log for suspicious activity. For each action, an audit log entry is created that includes the date and time, what type of event occurred, what user identification is associated with the event, and the outcome of the event. After completion of an auction, all data specific to the auction is deleted from the server by the auction services provider. BOEM will download and securely archive the audit log and will monitor records access to prevent unauthorized access. At BOEM, only authorized bureau personnel can access archived offshore energy lease sale records for official business purposes. Authorized BOEM personnel can access the downloaded and archived audit log for a completed auction at any point in time to support any investigations. Processes are in place to remove access to BAS and auction-related records for Federal employees and contractors who no longer have an official need-to-know.

All BOEM employees and contractors must complete Information Management and Technology (IMT) Awareness Training and the Information Systems Security ROB Acknowledgment before acquiring network and/or system access and annually thereafter. IMT Awareness Training includes modules on Cybersecurity, Privacy Awareness, Records Management, Section 508 Compliance, Controlled Unclassified Information, 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. Failing to protect PII or mishandling or misusing PII may result in disciplinary actions, the potential termination of employment, and criminal, civil, and administrative penalties.

GSA is responsible for protecting the data collected and processed on Login.gov. Login.gov manages security though the auditing of access, vetting of privileged users, enforcing the principle of least-privileged access, and maintaining strict control over the flow of information. 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. By using background check investigations for privileged users and individuals with access to user PII, 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. Additionally, all these managerial controls are subject to regular review. Login.gov's physical security is provided by its FedRAMP-authorized cloud service provider. Login.gov manages technological security via a defense-in-depth approach, minimizing access at every level, with strong encryption of data both in transit and at rest. Additionally, other services run on top of Login.gov to further detect any compromised systems, atypical system behavior, and/or data disclosure.

Treasury is responsible for protecting the data collected and processed on Pay.gov. Pay.gov maintains comprehensive security features that were designed into the interfaces and follows strict standards to effectively control risks posed by Internet threats, prevent web security vulnerabilities, and properly encrypt sensitive data stored within the database. Pay.gov uses software that can monitor network traffic and identify unauthorized attempts to cause damage or

upload or change information. Treasury implements access controls to ensure that access to PII maintained in Pay.gov is limited to individuals who have an official need-to-know the information in order to perform their official duties. Pay.gov maintains an audit log of system users to ensure they do not violate the system and/or Departmental/bureau rules of behavior.

Effective breach reporting procedures are essential to the rapid and effective resolution of breaches, mitigation of any potential harm to individuals and the agency, as well as to compliance with law and policy. Login.gov has an incident response plan and conducts incident and breach response exercises. Additionally, the system uses tools from the cloud service provider that heuristically detect both security incidents and potential breaches of PII. Third party services and agency partner systems that are integrated with Login.gov (such as BAS) are also required to report any breaches of information provided by Login.gov. Treasury maintains a breach response plan and notification policy, trains employees and contractors to protect PII, implements procedural safeguards to prevent the misuse of or unauthorized access to PII, and imposes accountability for failures to properly safeguard PII. All BOEM employees, contractors, detailees, interns, volunteers who have access to Federal information and information systems must immediately report a breach of PII in accordance with DOI policy and established procedures. This includes a suspected or confirmed breach in any medium or form, including paper, oral, and electronic. DOI and BOEM personnel also annually participate in tabletop exercises to test response plans, ensure incident response team members understand their roles and responsibilities, and identify any gaps or weaknesses.

The risk that BAS data will be maintained for longer than necessary is mitigated by BOEM's management of records in accordance with NARA-approved records schedules. After an auction's conclusion, the data associated with that auction is held in the system until BOEM has completed taking all required data for its records. After that point, and within 30 days of conclusion of the auction, all data is deleted from the BAS. BOEM downloads the files from the system, transmits them to DOJ for the required 30-day antitrust review, and then retains the files as Federal records in accordance with applicable Federal law. BOEM personnel who have an official need-to-know will have access to auction-related records. GSA and Treasury are responsible for mitigating privacy risk by maintaining Login.gov and Pay.gov records in accordance with NARA-approved records schedules.

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: BAS provides a secure, Internet-based solution for BOEM to conduct auctions of offshore energy leases. The data BOEM collects from companies seeking authorization to bid in a lease sale is both relevant and necessary to conducting auctions of offshore energy leases. The auction services provider uses the business-related PII shared by BOEM to provide representatives of companies authorized to bid in an auction with access to BAS. BAS users

provide Login.gov with consent to share their email address and agency-specific UUID with BOEM for authentication purposes.

☐ No

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

☐ Yes

☒ No: BAS does not derive or create new data that was previously unavailable about an individual through data aggregation. Login.gov may aggregate data on a user's device and behavior to detect and prevent identity impersonation or account takeover attempts. GSA maintains this information. BAS users may review the Login.gov PIA for information on how GSA may use aggregated user data.

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

☐ Yes

☒ No: BAS does not aggregate data. However, new user data derived by GSA through data aggregation may be placed in a Login.gov user's record. GSA maintains this information. BAS users may review the Login.gov PIA to determine if new user information derived from aggregated data will be placed in their Login.gov record.

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

☐ Yes

☒ No: Not applicable to BAS. To support user redress in suspected fraud and fraud investigations, Login.gov may match information within the Login.gov system and third-party fraud controls services to re-identify individuals. BAS users may refer to the Login.gov PIA for details about the types of information re-identified to support fraud investigations as permitted by the Login.gov SORN. Pay.gov sends transaction data that is necessary for fraud screening to third party vendors. Pay.gov users may refer to the Pay.gov PIA and Privacy and Security Policy for additional information.

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

BAS does not derive new data or create previously unavailable data about an individual through data aggregation.

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: Access to BAS is restricted to users who have valid login credentials. A user's access level is based upon their assigned user role.

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

Access to BAS is based upon assigned user roles. The only functions that a given user can access are those associated with that role. BAS is online only during specified periods (e.g., tests and scheduled auctions).

BOEM is responsible for 1) determining who has privileged access (e.g., Auction Managers and BOEM staff), 2) approving the list of bidders (companies) that can bid in the auction, and 3) sending the list of individuals authorized to bid on behalf of approved bidders to the auction services provider to facilitate their access to BAS for the auction.

BOEM publishes full bid results, including round-by-round results of the entire sale and exit bids, on its website after a review of the results and announcement of the provisional winner.

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 BAS or any associated records related to offshore energy leases.

Pay.gov roles and permissions enforce the principles of separation of duties and least privilege. Treasury deletes Pay.gov accounts after 396 days of inactivity. Users will receive an email notification after 365 days of inactivity that the agency will delete the account in 30 days if they remain inactive.

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: Contractors are involved with the design, development, and maintenance of the system. BOEM has worked with contracting officials to include the appropriate privacy clauses and terms and conditions 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: BAS has a robust audit log that captures all events undertaken by all users in the system.

Login.gov and Pay.gov log and monitor all user actions. Users may review the Login.gov and Pay.gov PIAs for additional information.

☐ No

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

The BAS audit log captures all transactions. For each action, an audit log entry is created including the date and time, what type of event occurred, what user identification the event is associated with, and the outcome of the event. During an auction, the Auction Manager team monitors the BAS audit log for suspicious activity.

All Login.gov traffic is subject to monitoring and recording to identify unauthorized attempts to change information or jeopardize the confidentiality, integrity, or availability of Login.gov. Users may review the Login.gov PIA for additional information.

Pay.gov uses software that can monitor network traffic and identify unauthorized attempts to cause damage or upload or change information. Users may review the Pay.gov PIA for additional information.

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

Monitoring of BAS is strictly limited to System Administrators and Auction Managers who review audit logs after each auction. In between auctions, the system is not online and cannot collect or process data.

All privileged non-bidding users such as Auction Managers must sign a rules of behavior form acknowledging their access responsibilities and the potential civil and/or criminal penalties that may result from a violation of BAS rules.

The BAS login screen features the required system use notification banner that provides privacy and security notices to system users. The banner clearly states all agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, facilitating protection against unauthorized access, and verifying security procedures, survivability, and operational security. It further states that, by logging into an agency computer system, the user acknowledges and consents to monitoring of the system. These security protocols help BOEM monitor user actions for appropriate use and to mitigate the risk of unauthorized monitoring.

Login.gov audits access, vets privileged users, and enforces principles of least-privileged access to decrease the risk of abuse. For Pay.gov, defined roles and permissions have been created to enforce the principles of separation of duties and least privilege. For additional information, users may review the Login.gov and Pay.gov PIAs.

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: Specific details regarding Amazon Web Services (AWS) US East / US West FedRAMP Moderate facility controls are described in the AWS System Security and Privacy Plan. The system also inherits controls from Login.gov for authentication. The Pay.gov PIA describes the physical controls implemented by Treasury to protect information processed using the service.

(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: Specific details regarding AWS US East / US West FedRAMP Moderate technical controls are described in the AWS System Security and Privacy Plan. The system also inherits controls from Login.gov for authentication. The Pay.gov PIA describes the technical controls implemented by Treasury to protect information processed using the service.

(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: Specific details regarding AWS US East / US West FedRAMP Moderate administrative controls are described in the AWS System Security and Privacy Plan. The system also inherits controls from Login.gov for authentication. The Pay.gov PIA describes the administrative controls implemented by Treasury to protect information processed using the service.

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 of the Economics Division in the Office of Strategic Resources is the BAS Information System Owner who is responsible for the oversight and management of the system and the implementation of adequate security and privacy controls. The Information System Owner and the Information System Security Officer, in consultation with the BOEM Associate Privacy Officer (APO), are responsible for complying with applicable Federal laws and policies to protect individual privacy and addressing any reported system- or process-related privacy issues in a timely manner.

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

Treasury is responsible for the management of Pay.gov, meeting the requirements of the Privacy Act and other Federal regulations, and protecting the privacy rights of individuals whose information is collected and processed on Pay.gov. DOI Pay.gov users are responsible for ensuring the proper management of records for their area of responsibility.

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 BAS Information System Owner has the responsibility for operational oversight and management of the system's security and privacy controls. The BAS Information System Owner and Information System Security Officer are responsible for ensuring that any suspected or confirmed loss, compromise, unauthorized disclosure, or unauthorized access to data is reported to the DOI Computer Incident Response Center (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. Agency partner systems like BAS that are integrated with Login.gov are also required to report any breaches or the compromise of 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, as well as for reporting upon discovery any potential loss, compromise, unauthorized access, or disclosure of data resulting from their activities or management of the data that may impact partner agencies in accordance with Federal policy and established procedures.

Treasury is responsible for managing the security of data collected and processed on Pay.gov, as well as for reporting upon discovery any potential loss, compromise, unauthorized access, or disclosure of data resulting from their activities or management of the data that may impact customer agencies in accordance with Federal policy and established procedures. DOI Pay.gov users are responsible for assuring proper use of the data they collect and reporting any loss, compromise, or unauthorized access or disclosure of information to the DOI-CIRC within 1-hour of discovery in accordance with the DOI Privacy Breach Response Plan and Federal policy and procedures, and for working with their respective Bureau APO to mitigate any impacts to individual privacy in accordance with the DOI Privacy Breach Response Plan.