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: Zoom for Government
Bureau/Office: Bureau of Ocean Energy Management (BOEM)
Date: June 10, 2020
Point of Contact:
Name: Melissa Allen
Title: BOEM Associate Privacy Officer
Email: boemprivacy@boem.gov
Phone: 202-208-7160
Address: 1849 C Street, NW, MS-OBPC, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?
   ☒ Yes, information is collected from or maintained on
     ☐ Members of the general public
     ☐ Federal personnel and/or Federal contractors
     ☐ Volunteers
     ☒ All

   ☐ No
B. What is the purpose of the system?

The mission of the Bureau of Ocean Energy Management (BOEM) is to manage development of U.S. Outer Continental Shelf energy and mineral resources in an environmentally and economically responsible way. Beyond internal collaborative efforts, BOEM programs often engage with external stakeholders and partners (i.e., members of the public; state, federal, Tribal, and local government agencies; members of Congress and/or their staff; industry representatives; and educational institutions) to fulfill the bureau's mission. In addition to in-person meetings, BOEM programs engage with internal and external stakeholders through a variety of digital services to enhance collaboration and transparency, such as services available on the Zoom for Government Platform.

The Zoom for Government Platform unifies cloud video conferencing, a cloud phone system, messaging, simple online meetings, and a software-defined conference room solution into one easy-to-use Platform. Zoom for Government Platform features include:

- **Zoom Cloud Video Conferencing**, a cloud-based collaboration service which includes video, audio, content sharing, and collaboration.
- **Zoom Phone**, a cloud-based phone system with traditional private branch exchange features, integrated public switches telephone network connectivity, enhanced emergency services, and support for calling from mobile apps, desktop apps, and legacy desk phone devices.
- **Zoom Chat**, a service that enables users to send chat messages in public or private channels organized by projects, teams, or topics as well as to share files, emojis, screenshots, and more.
- **Zoom Rooms**, software-based group video conferencing for conference and huddle rooms that run off-the-shelf hardware.
- **Zoom Room Connector**, a gateway allowing H.323 and Session Initiation Protocol systems to connect to Zoom meetings.
- **Zoom Meeting Connector**, a software version of the Zoom Cloud infrastructure intended for installation on the customer premise.
- **Zoom API**, which provides users with the ability for developers to easily add Video, Screen Share, and other features.

BOEM programs that are licensed to use the Zoom for Government Platform may use either one or a combination of the procured available features in accordance with established Rules of Behavior (ROB) and applicable federal and Department of the Interior (DOI) requirements.

Virtual meetings can greatly maximize public participation. However, BOEM's use of the Zoom for Government Platform is not intended to be an exclusive form of information dissemination and collaboration. BOEM programs (in applicable cases) will provide
alternate means of participation and access for individuals (e.g., toll-free teleconference lines and delivery of hard copies of meeting materials).

C. What is the legal authority?

Some legal authorities that authorize the use of the Zoom for Government Platform will be specific to the purpose of the program hosting the activity (e.g., the National Environmental Policy Act (NEPA) requires that agencies provide meaningful opportunities for public participation). BOEM programs using the Zoom for Government Platform will identify specific legal authorities in the notices they release pertaining their activities.


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 Zoom for Government is 010-000002297.
☐ No
F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

<table>
<thead>
<tr>
<th>Subsystem Name</th>
<th>Purpose</th>
<th>Contains PII (Yes/No)</th>
<th>Describe If Yes, provide a description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

☒ Yes: DOI has published the DOI-08, DOI Social Networks SORN, which covers communications with individuals who engage with DOI bureaus and offices through social media outlets and digital services.

Stakeholders may submit a comment or supporting materials on a BOEM rulemaking while participating in an official BOEM activity hosted on the Zoom for Government Platform. BOEM will maintain administrative records and comments, information, and documents received from the public as part of the public comment process through email correspondence, postal mail, or other methods (including, but not limited to, the Zoom for Government Platform) under the DOI-21, eRulemaking Program SORN.

DOI login credentials to access the Zoom for Government Platform is covered by DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS).

DOI SORNs are available for review on the DOI-Wide SORNs Web page.

☐ No

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
☒ Personal Email Address
☒ Employment Information
☒ Other: BOEM programs will typically either send stakeholders a direct invitation to attend an activity they are hosting through an official BOEM email or will request that interested participants pre-register to attend via a Web form or phone call to a contact specified in the press release for the activity.

The types of information BOEM programs may collect from interested participants will vary depending upon the purpose of the activity and needs of the participants. BOEM programs may collect the following types of information: Name, email address (personal or business-related), phone number (personal or business-related), title (business-related), and company/organization/agency (if applicable). BOEM programs will also collect the physical mailing address (personal or business-related) of interested participants who have requested hard copies of meeting materials.

BOEM programs remind interested participants not to provide sensitive PII or privileged information through direct notices (e.g., Privacy Notices provided at the time of registration and verbal reminders at the opening of meetings) and the BOEM Privacy Policy.

The BOEM Zoom Account Owner will verify the email addresses and requested privileges of approved BOEM program personnel prior to creating authorized user accounts for their bureau program. BOEM employees provide personal information and complete mandatory training in order to obtain login credentials to access the DOI network and systems (including, but not limited to, Zoom for Government) through the DOI Enterprise Active Directory.

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: Some of the individuals who provide PII to BOEM programs hosting an activity on the Zoom for Government Platform are representatives of external organizations or agencies. These representatives typically provide their non-sensitive, business-related PII to BOEM programs.
C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☒ Telephone Interview
☐ Information Shared Between Systems
☐ Other

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

BOEM programs will primarily collect PII from individuals to facilitate and manage an official BOEM activity on the Zoom for Government Platform. In some cases, BOEM programs may use PII to provide hard copies of meeting materials or other assistance in response to an individual’s request. When required by statute, BOEM programs will also use the collected PII to document meeting attendance and public comments as part of the public record for a project.

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

☒ Within the Bureau/Office: A BOEM program that is hosting an activity on the Zoom for Government Platform may share participant PII with other parties within BOEM when necessary to facilitate and manage the activity. Otherwise, BOEM personnel not involved with an activity will not have access to any participant information that BOEM does not make publicly available as part of public record.

☒ Other Bureaus/Offices: A BOEM program that is hosting an activity on the Zoom for Government Platform may receive assistance from other DOI bureaus and offices (e.g., Office of the Solicitor, Bureau of Safety and Environmental Enforcement, National Park Service, or the U.S. Fish and Wildlife Service) while responding to public comments. Other DOI bureaus and offices will not have access to any participant information that BOEM does not make publicly available as part of public record.

☒ Other Federal Agencies: A BOEM program that is hosting an activity on the Zoom for Government Platform may receive assistance from non-DOI federal agencies while responding to public comments. These federal agencies will not have access to any participant information that BOEM does not make publicly available as part of public record.
Tribal, State or Local Agencies: A BOEM program that is hosting an activity on the Zoom for Government Platform may receive assistance from tribal, state, or local agencies while responding to public comments. These agencies will not have access to any participant information that BOEM does not make publicly available as part of public record.

Contractor: Participant PII may become available to a contractor who is assisting a BOEM program that is hosting an activity on the Zoom for Government Platform. Contractors may also be involved in assisting a BOEM program in responding to public comments received during an official BOEM activity and maintaining the administrative record. These activities may provide contractors with access to participant information beyond what the BOEM program would make publicly available as part of public record.

Other Third Party Sources: BOEM programs using Zoom for Government to facilitate public comment periods through virtual public meetings may make limited participant information (e.g., name, affiliation (if applicable), and comment/question) publicly available as part of public record following the meeting. Some BOEM programs may also disseminate or make publicly available participant lists, depending on the nature and attendees of the meeting.

BOEM programs may receive Freedom of Information Act (FOIA) requests for participant lists and other activity-related materials. In these cases, the BOEM programs will coordinate with the BOEM FOIA Office to respond to the requests in compliance with the FOIA and DOI FOIA regulations. The BOEM FOIA Office will determine what information (if any) may be withheld from disclosure under one or more of the FOIA’s nine exemptions.

There may be unusual circumstances where user interactions indicate evidence of criminal activity, a threat to the government, a threat to the public, or a violation of Departmental policy. In these cases, information about the user interaction, including name, contents of interactions, and other personal information available to BOEM through Zoom for Government, may be used to notify the appropriate agency officials or law enforcement organizations as required by law.

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

Yes: Individuals interested in participating in a BOEM-hosted activity on the Zoom for Government Platform may decline to provide their information. In doing so, however, they may not be able to participate in the activity through the Platform. Individuals may, in some cases, be able to request to participate in an official activity in an alternate manner.
☐ No

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

☐ Privacy Act Statement

☒ Privacy Notice: BOEM programs will provide a Privacy Notice to stakeholders and interested participants when sending them an invite or collecting their information to facilitate and manage official BOEM activities on the Zoom for Government Platform. These Privacy Notices will include, but are not limited to, a brief description of how the BOEM program will handle participant PII, as well as a reminder that the BOEM Privacy Policy does not apply to the activities the bureau hosts on the Zoom for Government Platform. Participants will have access to links to Zoom for Government’s Privacy and Security policies. BOEM programs will coordinate with the BOEM Associate Privacy Officer to assess the adequacy of drafted Privacy Notices before using them to collect information.

☒ Other: At the start of any interactive activities being hosted on the Zoom for Government Platform, BOEM programs will remind participants not to share any sensitive PII or privileged information during the session without proper authorization.

BOEM programs using the Zoom for Government Platform to facilitate and manage part of a federal decision-making process (e.g., the NEPA process) will post opportunities for public participation on the BOEM.gov website, as well as place announcements in the Federal Register and/or in newspapers covering the potentially affected areas.

BOEM also provides notice through the publication of this PIA.

☐ 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 Zoom Account Owners centrally manage and monitor the authorized BOEM user accounts for their program and will typically retrieve data by authorized BOEM usernames, activity type (e.g., meeting or webinar), or activity title.

Authorized BOEM users will typically retrieve information on the Zoom for Government Platform by activity type or activity title.
I. Will reports be produced on individuals?

☑ Yes: BOEM does not produce reports on individuals but on the actions of authorized users. The Reports section is a powerful tool that provides BOEM Zoom Account Owners with various account, meeting, and webinar statistics for their bureau program. BOEM Zoom Account Owners will produce user activity reports, as necessary, to manage and monitor the activities of authorized BOEM users within their bureau program.

The Reports section also provides authorized BOEM users with the ability to review meeting statistics and registration/participant reports for their activities. Authorized BOEM users may export and maintain participant lists beyond the Platform to formally document the attendance of an official BOEM activity. The exported report may contain participant contact information.

☐ No

Section 3. Attributes of System Data

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

BOEM programs authorized to use the Zoom for Government Platform may collect contact information directly from interested participants and presume the collected information is accurate at the time of submission. Official stakeholder representatives and interested participants are responsible for providing BOEM programs with updated contact information, as necessary.

B. How will data be checked for completeness?

Interested participants who are providing information to pre-register to attend an official BOEM activity are responsible for providing with complete information.

When creating an authorized BOEM user account, the BOEM Account Owner will verify user information and permissions in accordance with established account procedures. The login of authorized BOEM Zoom for Government users onto the Platform is authenticated through the DOI Enterprise Active Directory.
C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

BOEM programs using the Zoom for Government Platform to host official activities may directly invite official stakeholder representatives or collect the contact information of interested participants in order to provide them with access to the activity. Stakeholders are responsible for ensuring that BOEM programs have their current information on file. Interested participants are responsible for providing accurate information at the time of submission and may contact BOEM to provide updated information, as necessary.

BOEM programs using the Zoom for Government Platform are responsible for coordinating account updates and the resolution of technical issues with their designated BOEM Zoom Account Owner. The login of authorized BOEM Zoom for Government users onto the Platform is authenticated through the DOI Enterprise Active Directory, which is kept current.

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

Retention periods for BOEM information maintained and hosted on the Zoom for Government Platform may vary, as BOEM programs approved to use the Platform will maintain records in accordance with the applicable records schedule specific to the content and context of the records.

In accordance with National Archives and Records Administration (NARA) Bulletin 2010-05, Guidance on Managing Records in Cloud Computing Environments, BOEM must ensure that all federal records stored on the cloud-based Zoom for Government Platform are readable and accessible throughout their respective life cycle.

The retention and disposition schedule of the user data that Zoom for Government maintains is authorized under Department Records Schedule-1, Administrative Records, 1.4-Information Technology (DAA-0048-2013-0001-0013 and DAA-0048-2013-0001-0014), which was approved by NARA. The disposition is temporary; cut-off when superseded or obsolete and destroy 3 years after cut-off.

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

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.

BOEM programs engage with internal and external stakeholders through a variety of digital services to enhance collaboration and transparency, including but not limited to, services available on the Zoom for Government Platform. The Zoom for Government Platform unifies cloud video conferencing, a cloud phone system, messaging, simple online meetings, and a software-defined conference room solution into one easy-to-use Platform.

With proper administrative configuration management, user awareness, and adherence to established ROB, Zoom for Government can serve as a risk-managed and accepted solution in support of creating and maintaining effective collaboration efforts between BOEM and stakeholder groups. The FIPS 199 security impact level is moderate and Zoom for Government services are offered in a FedRAMP-compliant cloud environment independent of the Zoom’s standard commercial cloud environment. Government information on the Zoom for Government Platform is managed and safeguarded in accordance with FISMA, Office of Management and Budget policies, NIST standards, and DOI security and privacy policies. The Zoom for Government Security Team is responsible for implementing the appropriate physical and technical safeguards to prevent unauthorized access to the Platform. Noted security features include, without limitation, secure socket layer encryption, AES 256-bit encryption, role-based user security, watermark screenshots, firewall compatibility, and a password-protected meeting option. BOEM programs are required to use the Zoom for Government Platform in accordance with applicable federal laws, regulations, and policies. There is a risk of unauthorized or inappropriate use of Zoom for Government by BOEM employees. To mitigate this risk, access to the Zoom for Government Platform is strictly limited to authorized personnel who require access to perform their official duties and users must not store or transmit unauthorized information on the Platform. All BOEM employees must complete privacy, Federal Information Systems Security Awareness (FISSA), and records management training prior to being granted access to DOI/BOEM information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. BOEM personnel also sign the DOI Rules of Behavior. All BOEM Zoom for Government users are responsible for abiding by the established Zoom for Government ROB to maintain a risk-managed balance between business and security requirements. BOEM users can log onto the Zoom for Government Platform through the DOI Enterprise Active Directory. BOEM Zoom Account Owners will centrally manage and monitor account usage of authorized users within their bureau program to enforce appropriate permissions and access levels. BOEM Zoom Account Owners will review user activity reports on a regular, periodic basis to address any
violations of the established ROB (such as storing or transmitting unauthorized information on the Zoom for Government Platform).

There is a risk that BOEM programs that are using the Zoom for Government Platform may collect more participant information than is necessary to accomplish their purpose or may use the collected information in an unauthorized manner. To mitigate these risks, BOEM Zoom Account Owners will restrict access to participant data, established ROB will require authorized personnel to not gather or store unnecessary information about individuals, and BOEM programs must coordinate with the BOEM Associate Privacy Officer to develop privacy notices that they will provide to interested participants and stakeholders when sending a meeting invite or collecting information for registration purposes. BOEM programs will also use the privacy notices to inform interested participants that the use of Zoom for Government services is subject to Zoom’s Privacy Policy; the BOEM Privacy Policy does not apply but BOEM programs will collect, maintain, use, disseminate, and dispose of PII in accordance with federal and DOI privacy requirements. BOEM programs are responsible for maintaining information on the Platform no longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. Any individuals who have privacy questions or complaints may contact the BOEM Associate Privacy Officer.

There is a risk that agency data and participant information may be disclosed to unauthorized individuals. The implementation of controls (physical, administrative, and technical), enforcement of security compliance protocol, and adherence to the established ROB will mitigate the risk of uninvited individuals joining an official BOEM activity on the Zoom for Government Platform and/or gaining unauthorized access to bureau and participant data. While most of the participant information will be comprised of the non-sensitive, business-related contact information of official stakeholder representatives, some participant information may pertain to members of the public. BOEM will not collect sensitive PII from participants and will remind participants to refrain from sharing sensitive or privileged information during official BOEM activities. In the event of a breach on the Zoom for Government Platform, the Zoom for Government Security Team will contact BOEM to report the breach. BOEM Zoom Account Owners and authorized BOEM users are required to immediately report any suspected or confirmed breaches of agency data. In either case, BOEM will follow procedures documented in the DOI Privacy Breach Response Plan. A privacy breach that results from a BOEM failure to protect PII or the mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.
Section 4. PIA Risk Review

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

☒ Yes, the use of the data is both relevant and necessary to facilitate and manage access to content hosted by BOEM programs on the Zoom for Government Platform during official activities.

☐ No

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

☐ Yes
☒ No

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

☐ Yes
☒ No

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

☐ Yes
☒ No

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

Not applicable, as new data is not being created.

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: BOEM programs will control participant access to the activities they host on the Zoom for Government Platform in accordance with the established ROB and security compliance requirements. Stakeholders participating in an official BOEM activity on the Zoom for Government Platform will have access only to BOEM-hosted content during the activity.

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

Each user in a BOEM program’s Zoom for Government account automatically has a system role (owner, user, or administrator). Roles are associated with a default set of permissions which cannot be changed. These permissions control what users see when they log into their account.

Each BOEM program using the Zoom for Government Platform will designate a Zoom Account Owner to serve as the program official responsible for the creation and management of user accounts for authorized program staff in accordance with documented account procedures. Authorized BOEM users can access only their account and the information stored in it to facilitate and manage their program’s official BOEM activities on the Zoom for Government Platform.

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, Privacy Act contract clauses have been included in contracts.

☐ 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. The Zoom for Government Platform provides BOEM Zoom Account Owners with the ability to centrally manage and monitor the activities of authorized BOEM users within their bureau program to prevent unauthorized use and support the implementation of federal and DOI requirements.

☐ No

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

All actions undertaken by BOEM personnel on the Zoom for Government Platform are recorded and available for review by authorized officials for auditing purposes. Authorized BOEM user actions include, but are not limited to, logins, hosted meetings, scheduled meetings, record deletions, and registration collections. BOEM Zoom Account Owner actions include, but are not limited to, creation of user accounts, deletion of user accounts, and modification of a user’s role privilege settings.

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

Access to the Zoom for Government Platform is provided only to authorized BOEM officials. The account permissions of BOEM Zoom for Government users will vary depending upon services contracted by BOEM programs, assigned user roles, and controls applied by BOEM Zoom Account Owners. BOEM Zoom Account Owners will centrally manage and monitor account usage of authorized users within their bureau program, as well as liaison with Zoom and appropriate bureau officials to resolve any observed or reported issues. Authorized BOEM users cannot make changes to their account permissions independent of their program’s designated BOEM Zoom Account Owner.

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. Zoom for Government is FedRAMP certified and is subject to the NIST Special Publication (SP) 800-53 security and privacy controls.

(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: Zoom for Government is FedRAMP certified and is subject to the NIST SP 800-53 security and privacy controls.

(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: Zoom for Government is FedRAMP certified and is subject to the NIST SP 800-53 security and privacy controls.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Information System Owner is the official responsible for overall oversight and management of the security controls and the protection of bureau information processed and stored on the Zoom for Government Platform. The Information System Owner and
BOEM Associate Privacy Officer, in collaboration with appropriate security officials, are responsible for ensuring safeguards are implemented to protect individual privacy in compliance with federal laws and policies for the data managed, used, and stored on the Zoom for Government Platform. BOEM Zoom Account Owners and authorized BOEM users are responsible for abiding by the established ROB and providing adequate privacy notices to individuals who choose to engage with BOEM on the Zoom for Government Platform. The BOEM Associate Privacy Officer is responsible for ensuring that authorized users understand and implement applicable privacy requirements, as well as for processing privacy complaints.

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 Information System Owner is responsible for the overall oversight and management of the security and privacy controls for BOEM use of the Zoom for Government Platform. All BOEM Zoom Account Owners and authorized BOEM users are responsible for complying with established ROB and federal and DOI requirements. The Zoom for Government Security Team will immediately contact the Information System Owner in the event of a data breach. The Information System Owner and BOEM users must report any potential or confirmed loss, compromise, unauthorized access, or disclosure of PII to the DOI Computer Incident Response Center (DOI-CIRC) within 1-hour of discovery in accordance with DOI policy and established procedures.