U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Zoom for Government Platform (Zoom)
Bureau/Office: Bureau of Safety and Environmental Enforcement (BSEE)
Date: December 3, 2020
Point of Contact:
Name: Rowena Dufford
Title: BSEE Associate Privacy Officer
Email: privacy@bsee.gov
Phone: 703-787-1257
Address: 45600 Woodland Road, Mail Stop: VAE-TSD, Sterling VA 20166

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on

- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No

B. What is the purpose of the system?

Zoom provides collaboration services through a cloud-based peer-to-peer software platform. The Zoom for Government Platform is FedRAMP approved, the features covered in this PIA are:

- **Zoom Cloud Video Conferencing**, a cloud-based collaboration service which includes video, audio, content sharing, and collaboration.
- **Zoom API**, provides developers the ability to easily add Video, Voice and Screen Sharing to the application. It helps manage the pre-meeting experience such as creating, editing and deleting resources like users, meetings and webinars.

The Department of the Interior (DOI) uses Microsoft Office 365 which is a line of subscription services offered as part of the Microsoft Office product line. It includes Teams which is the DOI-preferred collaboration platform. The features provided by Zoom, however, allow users to seamlessly facilitate and coordinate larger-scale, multi-day events and breakout sessions, allow for auto dial-in and enhanced control of participants which are not currently available on Teams. Zoom provides host-enabled interactive capabilities such as the use polling questions and active annotation by participants on shared screens or whiteboards. Sessions may be recorded as on-demand training or be viewed in the future by those who are given access to the recordings. Breakout sessions may request participants to voluntarily go on-camera as it appears to improve engagement.

The Bureau of Safety and Environmental Enforcement (BSEE) provides enterprise technical services to personnel at BSEE, the Bureau of Ocean Energy Management (BOEM) and the Office of Natural Resources Revenue (ONRR). Zoom will be available for use as an alternative enterprise application for collaboration with internal and external participants. BSEE Zoom user roles are administrator or hosts. Hosts may use the available features in accordance with the type of license purchased, established Zoom Rules of Behavior (ROB) for users and applicable federal and DOI requirements.

Specific uses beyond internal collaborative efforts include engagement by BOEM programs 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.

C. What is the legal authority?

Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012; Presidential Memorandum on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010; OMB Memorandum for the Heads of Executive Department Agencies, and Independent Regulatory Agencies, Social Media, Web-Based Interactive Technologies.

Some legal authorities that authorize the use of Zoom will be specific to the purpose of the hosted activity (e.g., the National Environmental Policy Act (NEPA) requires that agencies provide meaningful opportunities for public participation). For example, BOEM 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. Expanding the scope from BOEM only to BSEE Enterprise (BOEM, BSEE and ONRR)

E. Is this information system registered in CSAM?

☒ Yes: The UII code for Zoom for Government is 010-000002297 and is covered under the Zoom System Privacy Plan

☐ No

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

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

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

☒ Yes: 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. Training sessions are covered by DOI-16, Learning Management System. DOI login credentials to access Zoom is covered by DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS).

Specific uses by BOEM include having stakeholders submit a comment or supporting materials on a BOEM rulemaking while participating in an official BOEM activity hosted on Zoom. 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, Zoom) under the DOI-21, eRulemaking Program SORN.

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:

The BSEE Enterprise Zoom administrators will verify the email addresses and requested privileges of approved hosts prior to creating authorized accounts. The administrator and hosts create their own login ID and password credentials on Zoom.

The Zoom ROB requires hosts and presenters to remind 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 BSEE, BOEM or ONRR Privacy Policy as applicable.

The types of information that hosts may collect from participants will vary depending upon the purpose of the activity and the needs of the participants including those who have requested hard copies of meeting materials. Information can include: name, email address (personal or business-related), phone number (personal or business-related), title (business-related), company/organization/agency (if applicable), and physical mailing address (personal or business-related).

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 participants who provide PII are representatives of external organizations or agencies. These representatives typically provide their non-sensitive, business-related PII.

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?

Hosts and presenters will primarily collect PII from participants to facilitate and manage an official activity on Zoom. In some cases, PII may be used to provide hard copies of meeting materials or other assistance in response to a participant's request. When required by statute, 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 host may share participant PII with other parties within their bureau or office when necessary to facilitate and manage the activity. Participants will be able to see others attending a Zoom activity which may include their comments/questions. Other personnel not involved with an activity will not have access to any participant information that is not made publicly available as part of public record.

☒ Other Bureaus/Offices: Participant information may be shared with hosts and presenters from other Bureaus/Offices. A host may receive assistance from other DOI bureaus and offices (e.g., Office of the Solicitor, National Park Service, or the U.S. Fish and Wildlife Service) such as a presenter or while responding to public comments. Participants will be able to see others attending a Zoom activity which may include their comments/questions. Other DOI bureaus and offices will not have access to any participant information that is not made publicly available as part of public record.

☒ Other Federal Agencies: Participant information may be shared with hosts and presenters from other Federal agencies. A host may receive assistance from non-DOI federal agencies who may be acting as a presenter or while responding to public comments. Participants will be able to see others attending a Zoom activity which may include their comments/questions. These federal agencies will not have access to any participant information that is not made publicly available as part of public record.

There may be unusual circumstances where there is potential evidence of criminal activity, a threat to the government, a threat to the public, or a violation of Departmental policy. In these cases, information from the Zoom meeting, including name, contents of interactions, and other personal information available to BSEE, BOEM and ONRR through Zoom for Government, may be used to notify the appropriate agency officials or law enforcement organizations as allowed by law per established Routine Uses outlined in the applicable DOI SORNs.

☒ Tribal, State or Local Agencies: A host may receive assistance from tribal, state, or local agencies who may be acting as a presenter or while responding to public comments. Participants will be able to see others attending a Zoom activity which may include their comments/questions. These agencies will not have access to any participant information that is not made publicly available as part of public record.

☒ Contractor: Participant PII may become available to a contractor who is assisting with an activity on Zoom or acting as a presenter. Contractors participating will be able to see a list of participants and their interactions within a Zoom activity which may include their comments/questions.

Contractors are used for closed captioning services and to assist with 508-compliance for recorded, posted activities. They may also be involved in assisting a program in responding to public comments received during an official activity and maintaining the administrative record. These activities may provide contractors with access to participant information beyond what is made publicly available as part of public record.

☒ Other Third Party Sources: A host may receive assistance from third parties who may be acting as a presenter or while responding to public comments. Use of Zoom 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 hosted meetings may be required to disseminate or make publicly available participant lists, depending on the nature and participants of the meeting.

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

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

☒ Other: At the start of any interactive activity, hosts will remind participants not to share any sensitive PII or privileged information during the session without proper authorization. Notice will be given to participants before sessions are recorded. Hosts using Zoom to facilitate and manage part of a federal decision-making process (e.g., the NEPA process) will post opportunities for public participation on the Bureau/Office's official website, as well as place announcements in the Federal Register and/or in newspapers covering the potentially affected areas. Notice is also provided 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.).

Typically, data will be retrieved by the name of the host, activity type (e.g., meeting or webinar), or activity title. Authorized hosts can retrieve information on Zoom by activity type, title or occurrence.

I. Will reports be produced on individuals?

☒ Yes: The Zoom administrator can produce reports on the number of licenses, authorized hosts and their activities. Hosts can produce reports to review meeting statistics, registration and participant engagement. Hosts may export and maintain participant lists beyond the Platform to formally document the attendance of an official 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?

Hosts 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 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 activity are responsible for providing with complete information. When creating an authorized host account, the administrator will verify host information and permissions in accordance with established account procedures. The login of authorized hosts is authenticated directly through the Zoom for Government platform.

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

Hosts 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 programs have their current information on file. Interested participants are responsible for providing accurate information at the time of submission and may provide updated information, as necessary.

Hosts may create email distribution lists to facilitate invitations to attendees and must maintain their accuracy and limit to current, authorized members.

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 information maintained and hosted on Zoom may vary, as 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, must ensure that all federal records stored on the cloud-based Zoom are readable and accessible throughout their respective life cycle.

The retention and disposition schedule of the host 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.

Hosts 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 Zoom.

There is a risk that hosts may collect more participant information than is necessary to accomplish their purpose or may use the collected information in an unauthorized manner. There is also a risk such as when participants voluntarily go on-camera, participants may inadvertently show something on-screen that is not intended to be seen by others. This is mitigated through the ROB and educating hosts on the risk associated with use of Zoom. The ROB requires hosts to restrict access to participant data. Hosts must use the privacy notices available in the established Zoom procedures that they will provide to participants and stakeholders when sending a meeting invite, collecting information for registration, and prior to initiating the recording of a session. Hosts will also use the privacy notices to inform participants that the use of their information is subject to both Zoom for Government Privacy Policy and the respective bureau/office Privacy Policy. Hosts will collect, maintain, use, disseminate, and dispose of PII in accordance with

federal and DOI privacy requirements. Hosts 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 their respective Associate Privacy Officer.

There is a risk of unauthorized or inappropriate use of Zoom for Government by hosts. To mitigate this risk, access to Zoom is strictly limited to authorized personnel who require access to perform their official duties and hosts must not store or transmit unauthorized information on the Platform. All hosts must complete privacy, Information Management Training (IMT), and records management training prior to being granted access to agency, bureau/office 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. Personnel also acknowledge the DOI ROB. All Zoom for Government hosts are responsible for abiding by the established Zoom for Government ROB to maintain a risk-managed balance between business and security requirements. Hosts shall host Zoom activities with government furnished equipment. The Zoom Administrator will centrally manage and monitor authorized hosts accounts within BSEE Enterprise to enforce appropriate permissions and access levels. Zoom Administrator will review host activity reports on a regular, periodic basis to address any violations of the established ROB (such as storing or transmitting unauthorized information on Zoom).

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 activity on Zoom and/or gaining unauthorized access to bureau/office 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. Hosts will not collect sensitive PII from participants and will remind participants to refrain from sharing sensitive or privileged information during official activities. In the event of a breach on Zoom, the Zoom for Government Security Team will contact BSEE to report the breach. Zoom administrator or hosts are required to immediately report any suspected or confirmed breaches of agency data following procedures documented in the DOI Privacy Breach Response Plan. A privacy breach that results from a 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.

With proper administrative configuration management, host awareness, and adherence to established ROB, Zoom for Government can serve as an alternate, risk-managed and accepted solution in support of creating and maintaining effective collaboration efforts between BSEE, BOEM and ONRR and their 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 Zoom 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, transport layer security encryption, AES 256-bit encryption, role-based user security, watermark screenshots, firewall compatibility, and a password-protected meeting option. Hosts using the BSEE Enterprise Zoom for Government Platform are required to use it in accordance with applicable federal laws, regulations, and policies.

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: Yes, the use of the data is both relevant and necessary to facilitate and manage access to content hosted by programs on Zoom 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: Stakeholders participating in an official activity on Zoom will have access only to hosted content during the activity.

Hosts will control participant access in accordance with the established ROB and security compliance requirements.

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

Each user in a program's Zoom for Government account automatically has a system role (administrator or host). 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.

The Zoom administrator is responsible for the creation and management of user accounts for authorized hosts in accordance with documented account procedures. Hosts can access only their account and the information stored in it to facilitate and manage their official activities on Zoom.

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. The contract for the Enterprise Service Desk is ordered off the Government-wide Acquisition Contract and includes all privacy contract clauses by reference such as:

- 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
- 52.224-1, Privacy Act Notifications
- 52-224-3, Privacy Training
- 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a)

☐ 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 administrator will centrally manage and can monitor the activities of hosts to prevent unauthorized use in support 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 personnel on Zoom are recorded and available for review by authorized auditors. Authorized user actions include, but are not limited to, logins, hosted meetings, scheduled meetings, record deletions, and registrations. The Zoom administrator actions include, but are not limited to, creation of user accounts, deletion of user accounts, and modification of privileges.

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

Access to Zoom is provided only to authorized users. The account permissions of Zoom for Government users will be assigned by user roles, and controls applied by the Zoom administrator. The Zoom administrator will centrally manage and can monitor account usage of authorized users. Hosts cannot make changes to their account permissions.

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 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 Special Publication (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 Zoom. The Information System Owner and respective 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 Zoom. Hosts are responsible for abiding by the established ROB and providing

adequate privacy notices to individuals who choose to engage on Zoom. Each respective 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 the use of Zoom. The Zoom administrator and hosts 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 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.