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
Bureau/Office: Bureau of Land Management
Date: January 22, 2025
Point of Contact
Name: Jamie Huang
Title: Associate Privacy Officer
Email: BLM_HQ_Privacy@blm.gov
Phone: 301-873-1132

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?

Department of the Interior (DOI) bureaus and offices use various approved digital tools to assist in communicating with internal and external stakeholders. Zoom for Government ("Zoom" or "Platform") is a cloud-based Software as a Service (SaaS) platform that unifies cloud video conferencing, simple online meetings, and a software-defined conference room solution into one platform. The solution offers video, audio, and wireless screen-sharing across various types of

electronic devices and operating systems. This PIA describes the use of Zoom by the Bureau of Land Management (BLM). BLM provides enterprise technical services to personnel and is responsible for information technology security policy and operational support.

The Zoom features available to enterprise users depend on their assigned user role. Licensed BLM Zoom users are assigned a user role (administrator or member, referred to herein as "host") by the BLM Zoom Administrator. Zoom enables users at BLM to host single sessions, large-scale multi-day events, and breakout rooms with both internal and external stakeholders. Hosts may record sessions for on-demand viewing by authorized viewers. Zoom also provides host-enabled interactive capabilities such as polling questions and active annotation by participants on shared screens or whiteboards. Participants do not need to have a Zoom account to attend an official activity hosted by BLM.

C. What is the legal authority?

The legal authorities that authorize the use of Zoom include 5 U.S.C. § 301, Departmental Regulations; 44 U.S.C. § 3301, Federal Records Act; Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012; Presidential Memorandum on Transparency and Open Government, January 21, 2009; Office of Management and Budget (OMB) Memorandum M-10-06, Open Government Directive, December 8, 2009; OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010; and OMB Memorandum on Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act, April 7, 2010.

Other legal authorities that authorize the use of Zoom are 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). BLM hosts will identify specific legal authorities in the notices they provide to participants pertaining to the activities they host on the Platform and are responsible for ensuring that their use of Zoom falls within relevant authorities, law, and policy.

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 Bison Governance, Risk, and Compliance (GRC) platform?

☒ Yes: The BLM Zoom for Government System Security Privacy Plan (SSPP) is being developed. The approved SSPP will be posted in the Bison GRC.

☐ 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: While BLM typically does not use Zoom to maintain records retrieved by name or other personal identifiers, some information created through their use of Zoom may be incorporated into agency records subject to the Privacy Act. Where information is collected into, maintained as part of, or used or disseminated from a system of records, such collection, use, maintenance, and dissemination will be conducted in accordance with the Privacy Act of 1974 and consistent with the relevant SORN. The types of information potentially collected, used, and shared using Zoom may be covered under several applicable DOI SORNs that are available for review on the DOI SORN website at https://www.doi.gov/privacy/sorn:

- DOI has published INTERIOR/DOI-08, DOI Social Networks - 76 FR 44033 (July 22, 2011); modification published 86 FR 50156 (September 7, 2021), which covers communications with individuals who engage with DOI bureaus and offices through social media outlets and digital services.

- Records created through the use of Zoom to conduct training sessions are covered by INTERIOR/DOI-16, Learning Management System - 83 FR 50682 (October 9, 2018).

- Single sign-on (SSO) allows users to log into Zoom using their organization credentials and login information. DOI login credentials used to access Zoom are covered by INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - 72 FR 11040 (March 12, 2007); modification published 86 FR50156 (September 7, 2021).

- Specific uses of Zoom that are related to rulemaking may create records that are covered by INTERIOR/DOI-21, eRulemaking Program - 85 FR 33701 (June 2, 2020).

☐ No

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

☐ Yes:

☒ No: Hosts that plan to use Zoom to conduct activities under the Paperwork Reduction Act (PRA) are responsible for coordinating with their respective Information Collection Clearance Officer to ensure that their information collection activities adhere to the requirements of the PRA, OMB directives, and other applicable legislation.

Section 2. Summary of System Data

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

In all instances, a BLM Zoom session *could* collect:

☒ Name
☒ Email Address
☒ Employment Information
☒ Other: Information is collected from bureau/office hosts and internal and external meeting participants.

The BLM Enterprise Zoom Administrator will verify an approved bureau/office host's email address and requested account privileges prior to creating an authorized account. BLM hosts will log into Zoom using their DOI login credentials.

Given the varied nature of DOI's work and the potential uses of collaborative Platforms, Zoom may contain additional information during official activities hosted using the Platform. However, BLM Zoom users will only collect the minimum information necessary to conduct official activities on the platform. The Zoom meeting hosts may generally request for information from individuals for registration purposes including, but is not limited to, their name, email address (personal or business-related for external participants and business-related for internal participants), title (business-related, if applicable), and company/organization/agency (if applicable). A phone number may be requested in limited cases for an authorized purpose (internal participants will generally provide their business-related phone number: external participants may provide either their personal or business-related phone number). Participants may also provide additional personal information while submitting an accommodation request.

When joining an official activity hosted by BLM, participants can opt to display their real name or customize their displayed screen name. Depending on the nature of the hosted session and participant-managed permissions, a participant's Zoom profile photo, voice, and real-time video may become available to the host and/or other participants. Participants can also enter any kind

of information in open fields (e.g., Chat and Q&A) which may implicate other types of personal information, including but not limited to race, ethnicity, citizenship, and gender.

Zoom generates and/or collects information relating to hosted official activities (e.g., total meeting time, date, start time, end time, topic, participants, meeting ID, session ID, other metrics about when and how meetings were conducted, and what features were used), performance data (e.g., relating to how the services perform), service logs (e.g., relating to information on system events and states), and other operational information or metadata. Zoom also uses information about the types of devices and systems used by participants (e.g., computer type, speaker, microphone, operating system, average bandwidth) to facilitate a seamless participant meeting experience and help ensure the participant's desired configurations are used in the meeting experience.

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: Information is collected from BLM hosts and meeting participants.

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: *Describe*

Zoom leverages SAML 2.0 for SSO with DOI login credentials. DOI Active Directory is used to identify and authenticate users to the system.

☒ Other: *Describe*

Information is collected from and/or made available by BLM hosts and internal/external meeting participants during official activities hosted on the Platform.

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

Hosts will primarily collect PII from individuals 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: The BLM Zoom Administrator can access meeting, host, and participant information for management and oversight purposes. BLM hosts can access information for meetings that they hosted on the Platform. Depending on the nature of the session and participant permissions, PII may become available to bureau/office participants during an official activity. BLM hosts may share Zoom records and meeting recordings with personnel and/or meeting participants within each bureau/office for lawful and appropriate purposes.

☒ Other Bureaus/Offices: Depending on the nature of the session and participant permissions, PII may become available to participants in other bureaus/offices during an official activity hosted by BLM. Participant information may become available to other DOI bureaus and offices that are assisting hosts and/or while responding to public comments. BLM hosts may share Zoom records and meeting recordings with personnel and/or meeting participants in other DOI bureaus and offices for lawful and appropriate purposes.

☒ Other Federal Agencies: Depending on the nature of the session and participant permissions, PII may become available to participants in other Federal agencies during an official activity hosted by BLM. Participant information may become available to other Federal agencies that are assisting hosts and/or while responding to public comments. BLM hosts may share Zoom records and meeting recordings with personnel and/or meeting participants in other Federal agencies for lawful and appropriate purposes.

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 may be used to notify the appropriate agency officials or law enforcement organizations as allowed by law per the established routine uses outlined in the applicable SORN(s).

☒ Tribal, State or Local Agencies: Depending on the nature of the session and participant permissions, PII may become available to participants in Tribal, state, and local agencies during an official activity hosted by BLM. Participant information may become available to Tribal, state, and local agencies that are assisting hosts and/or while responding to public comments. BLM hosts may share Zoom records and meeting recordings with personnel in Tribal, state, and local agencies for lawful and appropriate purposes.

☒ Contractor: Depending on the nature of the session and participant permissions, PII may become available to contractor participants during an official activity hosted by BLM. Participant information may become available to contractors who are assisting BLM hosts with an official activity hosted on the Platform. Contractors may be involved in assisting a program in responding to public comments received during an official activity and maintaining the administrative record. Contractors are also used for closed captioning services and to assist with Section 508 compliance for recorded and posted activities. BLM hosts may also share Zoom records and meeting recordings with contractors for lawful and appropriate purposes.

☒ Other Third Party Sources: Depending on the nature of the session and participant permissions, PII may become available to members of the public who participate in an official activity hosted by BLM. BLM hosts may share Zoom records and meeting recordings with members of the public for lawful and appropriate purposes.

BLM may receive Freedom of Information Act (FOIA) requests for participant lists and other official activity-related records. The respective Bureau/Office FOIA Office will process the requests in compliance with the FOIA and DOI FOIA regulations.

Zoom has access to BLM data stored on the Platform and employs role-based access controls to prevent unauthorized access and disclosure.

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

☒ Yes: Using Zoom to host a meeting is voluntary. BLM personnel who request Zoom for Government accounts are required to provide their business-related contact information to use the Platform. The BLM Zoom Administrator will verify host information and permissions when creating an authorized host account. The login of authorized hosts is authenticated using DOI login credentials. Without consenting to provide their information, personnel will not be granted an authorized host account.

Internal and external individuals interested in participating in an official activity on Zoom hosted by BLM may decline to provide their requested information to the hosting bureau or office. In doing so, however, they may not be able to participate in the activity through the Platform. In some cases, individuals may be able to request to participate in an official activity in an alternate manner (e.g., listening to meeting audio through a provided teleconferencing number).

Participants have the option to customize their displayed screen name to preclude identification and can control whether to share their video and audio if the host has not disabled those functions.

Participants are notified whenever a meeting will be recorded and can leave the meeting or mute their audio and/or video to avoid having their voice and/or likeness recorded. Users may voluntarily participate in chat communications with the understanding that such communications

(unless directed privately to another user) may be available for viewing by other users and may be logged/transcribed by other users and/or the system.

While providing a public comment during an official activity hosted on Zoom, participants can ask the hosting bureau or office to withhold their PII from public review, but the hosting bureau or office cannot guarantee that it will be able to do so.

☐ No

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

☒ Privacy Act Statement: Hosts will provide a Privacy Act Statement to participants when requesting participants to provide personal information about themselves which will go into a system of records. Hosts must coordinate with the BLM Associate Privacy Officer (APO) to assess the adequacy of drafted Privacy Act Statements before using them to collect information. When drafting a Privacy Act Statement, hosts must include the legal authority for collecting the information (i.e., statute, executive order, regulation), the purpose(s) for collecting the information and how BLM will use it, to whom BLM may disclose the information outside of the agency and for what purposes, whether providing the information is mandatory or voluntary, and the effects of not providing the requested information.

☒ Privacy Notice: A Privacy Notice is required when PII is present or collected but may not necessarily be maintained in a Privacy Act system. Hosts must coordinate with the BLM APO to assess the adequacy of drafted Privacy Notices before using them to collect information. A Privacy Notice has the same requirements as a Privacy Act Statement and must include the authority and purpose for collecting the information, uses of the information, any sharing or dissemination of the information, and the consequences of not providing the information.

Where information is collected into, maintained as part of, or used or disseminated from a system of records, such collection, use, maintenance, and dissemination will be conducted in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and consistent with the applicable SORN. Government-wide SORNs maintained by other agencies may be viewed on the Federal Privacy Council Government-wide SORNs Web page. Links to DOI-wide and Bureau and Office Privacy Act SORNs are accessible through the Privacy Act System of Records Notices Web page maintained by the DOI Privacy Office.

Notice is also provided through the publication of this PIA on the BLM PIA Web page maintained by the DOI Privacy Office.

☒ Other: Prior to the start of a live meeting, hosts will provide participants with a notice that information may be collected for U.S. Federal Government-authorized use and remind them not to share any sensitive PII or privileged information without proper authorization. Hosts will also provide participants with a clear advance notice if a meeting will be recorded. Participants can leave the meeting or mute their audio and/or video to avoid having their voice and/or likeness

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 official website of the respective bureau or office, as well as place announcements in the Federal Register and/or in newspapers covering the potentially affected areas.

The Zoom Rules of Behavior (ROB) require hosts and their co-hosts to remind participants not to share sensitive PII or privileged information while attending a session through direct notices (e.g., Privacy Notices provided at the time of registration and verbal reminders at the opening of meetings). Participants may also review the Zoom Privacy Statement and DOI Privacy Policy.

☐ 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, the BLM Enterprise Zoom Administrator will retrieve data by the name of a host, activity type (e.g., meeting or webinar), or activity title.

Hosts can retrieve information on Zoom that pertain to their use of the Platform by activity type, title, or occurrence (i.e., single-session or recurring session).

I. Will reports be produced on individuals?

☒ Yes: The BLM Enterprise Zoom Administrator can produce reports on the number of issued licenses and 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 information (e.g., name and email address).

Audit logs are generated to document user access and activity within the System, which may contain details relating to the use of the system, including username, date/time, user's last date of login, failed login attempts, data/reports accessed, and data exported.

☐ No

Section 3. Attributes of System Data

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

Hosts who collect information directly from participants presume that the collected information

is accurate at the time of submission. Participants are responsible for providing the hosting bureau or office with accurate information, as necessary.

B. How will data be checked for completeness?

When creating an authorized BLM host account, the BLM Zoom Administrator will verify host information and permissions in accordance with established account procedures. The login of authorized hosts is authenticated using DOI login credentials. As a function of Active Directory, all data related to user access is continuously synchronized across the enterprise.

Individuals who are providing information to register to attend an official activity are responsible for providing hosts with complete information. Hosts can require the completion of registration fields to prevent incomplete submissions of registration information.

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

The BLM Enterprise Zoom Administrator reviews the configuration of Zoom on a regular, periodic basis in accordance with established procedures to review account access and enable, modify, or disable account access. The login of authorized BLM hosts is authenticated using DOI login credentials. As a function of Active Directory, all data related to user access is continuously synchronized across the enterprise.

Individuals are responsible for providing current information at the time of registration and must provide updated information to the hosting bureau or office, as necessary.

Hosts may create and maintain email distribution lists to facilitate invitations to recurring meeting participants and must maintain the accuracy of their lists to limit official activity access to authorized participants.

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

Common records that may be created through collaboration platforms such as Zoom include shared documents, chats, and meeting recordings. In accordance with National Archives and Records Administration (NARA) Bulletin 2023-04, NARA expects Federal agencies using collaboration platforms to manage the records they create according to their approved records schedules.

Agencies should follow the same established records management policies for documenting decisions or other substantive conversations during a video conference as they would for an in-person meeting. The Federal Records Act requires agencies to create adequate and proper documentation of their activities. The content of a meeting recording determines its retention. Meeting recordings with significant value must be maintained in accordance with an applicable agency-specific schedule.

Agencies participating in a collaboration platform like Zoom should designate records management responsibilities prior to working together. Ideally, the agency providing the collaboration platform is responsible for managing records for all participants in the platform. If this is not practical, the providing agency should make the records available to all participating agencies. Agencies also need to consider responsibilities when inviting new agencies to participate in the collaboration platform. Agencies may choose to use a Memorandum of Understanding to further clarify the records management roles and responsibilities for collaboration platform participants.

The retention of the user data that Zoom 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. System Maintenance and Use records (DAA-0048-2013-0001-0013) are cut off when superseded or obsolete and destroyed no later than 3 years after cut-off. System Planning, Design, and Documentation records (DAA-0048-2013-0001-0014) are cut off when superseded by a newer version or upon termination of the system and destroyed 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 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.

With proper administrative configuration management, host awareness, and user adherence to established ROB and privacy policies and procedures, Zoom can serve as an alternate risk-managed and accepted solution in support of effective engagement with internal and external stakeholders.

The Zoom for Government Federal Information Processing Standards (FIPS) Publication 199 security impact level is Moderate and Platform services are offered in a FedRAMP-compliant cloud environment independent of Zoom's standard commercial cloud environment. Government information on Zoom is managed and safeguarded in accordance with the Federal Information Security Modernization Act (FISMA), OMB policies, and National Institute of Standards and Technology (NIST) standards. Noted Zoom security features include 256-bit AES-GCM encryption, optional end-to-end encryption for Zoom Meetings, advanced Team Chat encryption, image and audio watermarking, and a passcode-protected meeting option.

The BLM Enterprise Zoom Administrator will verify an approved host's email address and requested privileges prior to creating an authorized account. Permissions and privileges are role-based to ensure that a host's capabilities on the Platform are limited to what is necessary. All bureau/office personnel (including hosts) 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 (CUI), and the PRA. 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.

Approved hosts are required to use the service in accordance with applicable Federal laws, regulations, policies, and DOI requirements. All BLM hosts are also responsible for abiding by the established Zoom for Government ROB to maintain a risk-managed balance between business and security requirements and shall host official activities using government furnished equipment. Despite these controls, there is a risk of unauthorized or inappropriate use of Zoom by hosts. The BLM Enterprise Zoom Administrator will centrally manage and monitor authorized host accounts to enforce appropriate permissions and access levels. The BLM Enterprise Zoom Administrator will also 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). Annual IMT Awareness Training, annual role-based training, and ad hoc privacy and security awareness campaigns will help reinforce the requirement to use approved services in accordance with established ROB and applicable Federal and Departmental requirements.

There is a risk that participants will not receive adequate notice about the collection and use of their information. Hosts may also collect more participant information than is necessary to accomplish their purpose. Hosts are responsible for providing internal and external participants with a Privacy Notice or Privacy Act Statement when posting or sending a meeting invitation, collecting information for registration, and prior to initiating the recording of a session. Hosts are limited to using collected information for the purpose described in the Privacy Notice or Privacy Act Statement. While reviewing Privacy Notices and Privacy Act Statements drafted for official activities on Zoom, the respective Bureau/Office APO will verify that a proposed notice complies with Federal and DOI requirements. Annual IMT Awareness Training, annual role-based privacy training, and ad hoc privacy awareness campaigns will help reinforce the requirement to collect the minimum information necessary to carry out an authorized business purpose and provide a Privacy Notice or Privacy Act Statement to individuals at the point of collection.

BLM hosts and meeting participants may share PII about themselves or others during virtual meetings, whether verbally, through chat or direct messaging, or while sharing their video, audio, or other information on their screens or their applications. Hosts are also responsible for vetting the releasability of bureau/office information they may share with participants. To further mitigate the risk of unauthorized access to PII and the potential subsequent misuse of PII, hosts may limit meeting attendance by adding a passcode for additional security or creating a “waiting room” where invitees must wait until the meeting host allows them to join the session, provide notices or make announcements recommending that participants limit their disclosure of

extraneous PII, and limit the Zoom features available during the official activity to manage participation (e.g., disabling the chat function, refusing screen sharing requests, and disabling the audio and video functions).

The BLM Enterprise Zoom Administrator and users are required to immediately report any suspected or confirmed breach of PII in accordance with DOI policy and established procedures. 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. Zoom will contact BLM if it detects a breach on the Platform.

There is a risk that hosts may maintain records longer than prescribed by NARA-approved records schedules. Hosts must 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. Bureau/Office Records Officers must work with the BLM Zoom Administrator and BLM hosts to perform a risk-based analysis of how they intend to use Zoom and ensure recordkeeping requirements are identified and met. Compliance with records management requirements to mitigate this risk is reinforced through annual records management training, Bureau/Office Records Management Program oversight and guidance, system rules for data management, and making sure bureaus and offices have adequate resources to implement the related applicable security and privacy controls.

Hosts and internal and external stakeholders who have privacy questions or complaints may contact the responsible Bureau/Office APO. APOs are responsible for managing and overseeing privacy program activities within their respective bureaus and offices to ensure compliance with Federal privacy laws and policies and Departmental requirements in alignment with the DOI Privacy Program and under the oversight of the SAOP and DPO.

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 participating 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: *Describe*

Hosts will control participant access to information in accordance with the established ROB and security compliance requirements. Internal and external meeting participants have access to content hosted on the Platform during the official activity.

Participant information may become available to contractors who are assisting BLM hosts with an official activity hosted on the Platform. Contractors may be involved in assisting a program in responding to public comments received during an official activity and maintaining the

administrative record. Contractors are also used for closed captioning services and to assist with Section 508 compliance for recorded and posted activities.

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

Each user in a bureau/office 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 can access when they log into their account.

The BLM Enterprise 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 appropriate privacy Federal Acquisition Regulation clauses and terms and conditions are included in the contract. Contractors who support official bureau/office activities hosted on Zoom are subject to information security, privacy, and other provisions in their contract binding them under the Privacy Act and other applicable laws.

☐ 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 BLM Zoom Administrator centrally manages roles assigned to authorized users such as hosts and monitors their activities to prevent unauthorized use in support of compliance with applicable Federal laws, regulations, policies, 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 host actions include, but are not limited to, logins, hosted meetings, scheduled meetings, record deletions, and registrations. BLM Enterprise 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?

The account permissions of authorized Zoom for Government users are conferred by assigned user roles and controls applied by the BLM Enterprise Zoom Administrator who centrally manages roles assigned to authorized users and can monitor their account usage. Hosts have no administrative privileges and cannot make changes to their account permissions.

All personnel must complete initial and annual IMT Awareness Training and the Information Systems Security ROB Acknowledgment. IMT Awareness Training includes modules on Cybersecurity, Privacy Awareness, Records Management, Section 508 Compliance, CUI, and the PRA. 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.

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 subject to 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 subject to 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 subject to 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 BLM Enterprise Operations Chief in the Enterprise Operations & Support Branch is the Information System Owner and the official responsible for overall oversight and management of the security controls and the protection of information processed and stored on the Platform. The Information System Owner and respective Bureau/Office APO, in collaboration with the appropriate security officials, are responsible for ensuring safeguards are implemented to protect individual privacy in compliance with Federal laws, regulations, 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 with their bureau or office on Zoom. Each Bureau/Office APO is responsible for ensuring that authorized users within their organization understand and implement applicable privacy requirements, as well as for addressing Privacy Act requests and privacy complaints in a timely manner.

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 BLM Enterprise Zoom Administrator and hosts are responsible for complying with established ROB and applicable Federal laws, regulations, policies, and DOI requirements. The Information System Owner and users must report any suspected or confirmed loss, compromise, unauthorized access, or unauthorized 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. The Information System Owner must also coordinate with the APO for the impacted bureau or office to mitigate any impact to individuals resulting from a breach in PII in accordance with the DOI Privacy Breach Response Plan and the BLM Incident Handling Procedures. Zoom will contact BLM if it detects a breach on the Platform.