

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

Please submit your responses to your Liaison Privacy Official. *All entries must be Times New Roman, 12pt, and start on the next line.* If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Zoom for Government (ZoomGov) Conferencing		
Preparer: Lauren Harris	Office: OMS/OITO/DCSB	
Date: 1/09/2023	Phone: 202-566-2265	
Reason for Submittal: New PIA_____ Revised PIA_____ Annual Review_X_ Rescindment _____		
This system is in the following life cycle stage(s):		
Definition <input type="checkbox"/>	Development/Acquisition <input type="checkbox"/>	Implementation <input type="checkbox"/>
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>		
<p>Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u></p> <p>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</u></p>		

Provide a general description/overview and purpose of the system:

Zoom for Government (ZoomGov) is a FedRAMP approved Software-as-a-Service (SaaS) Cloud-based conferencing service stored in AWS GovCloud maintained specifically for use by US Government users featuring ZoomGov Meetings and Chat, ZoomGov Video Webinar and ZoomGov Phone which allows participants to communicate as a group through use of audio and video and content sharing.

ZoomGov has all the same features within Zoom Commercial (Publicly offered Zoom service) but operates in a dedicated, secure infrastructure designed to meet the requirements of FedRAMP Moderate baseline and DOD Impact Level 2.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

The specific legal authority for this collection of information is 5 U.S.C. 301 “Departmental Regulations”, 8 U.S.C 1101, 1103, 1104, 1201, 1255, 1305, 3101 “Records Management by Federal Agency Heads.”

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes- Signed on September 29, 2020. ATO will expire on September 22, 2023.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required. ZoomGov is not covered by the Paperwork Reduction Act.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes. ZoomGov data is stored in the AWS GovCloud.
ZoomGov is a FedRAMP approved SaaS.

<https://www.zoomgov.com/> (Generic URL)

<https://www.usepa.zoomgov.com/>
(Possible custom EPA URL after implementation)

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The ZoomGov service typically included the following information for each user:

- Account Type - (e.g. Pro, Business, Enterprise) – EPA will be purchasing Enterprise type licenses

- Account Name - (e.g. Bob Smith)
- Account Alias (e.g. Bob's account for seminars)
- Role: (e.g. Member, Admin, etc)
- Account Owner: Email Address
- Account # - ZoomGov generated #
- Meeting Capacity: the default number of attendees permitted for each call

None of the above information is accessible or can be searched under a user's access, except for the name of an individual in order to invite or connect.

2.2 What are the sources of the information and how is the information collected for the system?

EPA will designate several account managers (Federal and Contractor staff) that will be able to assign licenses owned by EPA to users. These licenses will be assigned to users only upon a formal request from approved EPA federal staff.

EPA's ZoomGov account managers will use data from other EPA data sources such as National Locator and MS Active Directory to collect information from ZoomGov users for the purpose of provisioning accounts and to help facilitate and manage EPA activity on the ZoomGov Platform .

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ZoomGov does NOT use information from any commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

EPA has developed and implemented an Enterprise Identity Data Warehouse (eIDW) that is used for the provisioning and deprovisioning of users. This eIDW has structured arrangement where an authoritative data source is established for each data element and that data is replicated to other sources.

ZoomGov licenses do allow information to be collected for the purpose of provisioning users. Due to the nature of the system and the anticipated broad use of these services across the EPA, it is the responsibility of each user to ensure the accuracy of data at the time the data is created or used. System administrators ensure user information is accurate through a user request form submitted by the users and through authentication with the EPA Active Directory (AD) service and will not ensure accuracy of any specific data created or entered by the end users. EPA is implementing Single Sign-on and will use EPA's Enterprise Authentication service to validate EPA user log in.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Because ZoomGov contains the names of individuals, email, and phone numbers, there is a very low risk that this type of PII could be viewed or captured by unauthorized individuals. This makes it possible that the information could be used for social engineering purposes if divulged and could cause an intruder or unauthorized individual the ability intercept or join a meeting they are not authorized to attend.

Mitigation:

ZoomGov protects the information through defense-in-depth security controls that can only be accessed by a few dedicated administrators that directly administrate and manage the system. Some of these security controls are:

- Limiting the host of ZoomGov sessions as the only person authorized to use this information for setting up the meetings.
- Access is strictly limited to authorized personnel who require access to perform their official duties and users must not store or transmit unauthorized information
- All employees must complete Information Security and Privacy Awareness Training (ISPAT) and Records Management training prior to being granted access to ZoomGov.
- 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.
- All personnel also must sign the EPA Rules of Behavior.
- Any guest or individual not signed into meeting is identified and will show in the participants list with an orange background behind their names.
- Training users to avoid sharing meeting links on social media or public outlets or using Personal Meetings ID (PMI) to host public events.
- Restricting the sharing to of screens to only the host.
- Managing participants by locking the meeting after the meeting has started, so no new participants can join.
- Requiring participants to sign up for larger meetings and a short time before the meeting, send the password and link to all registrants.
- Utilizing the waiting room feature which is a virtual staging area that stops guests

from joining until the host is ready for them.

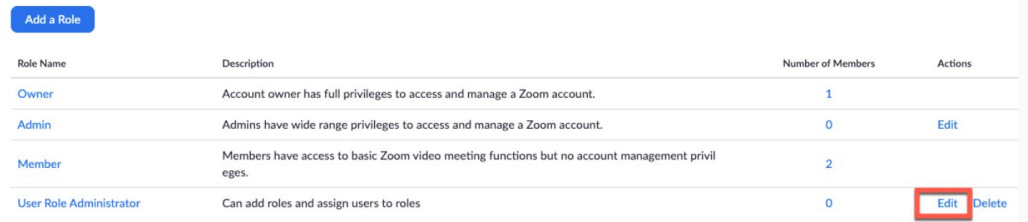
Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes. Each user must have a ZoomGov account and automatically has a system role, which can be either an owner, administrator, member or user role administrator. These roles are associated with a default set of permissions, which cannot be changed for the owner or member. These permissions control what users can access and/or do when they sign into the web portal. Role-based access control enables your account to have additional user roles. User roles can have a set of permissions that allows access only to the pages a user needs to view or edit. In addition, you can change the permissions of administrator system role.

Each user will belong to one of the roles below, and different roles have their unique privilege.



Role Name	Description	Number of Members	Actions
Owner	Account owner has full privileges to access and manage a Zoom account.	1	
Admin	Admins have wide range privileges to access and manage a Zoom account.	0	Edit
Member	Members have access to basic Zoom video meeting functions but no account management privileges.	2	
User Role Administrator	Can add roles and assign users to roles	0	Edit Delete

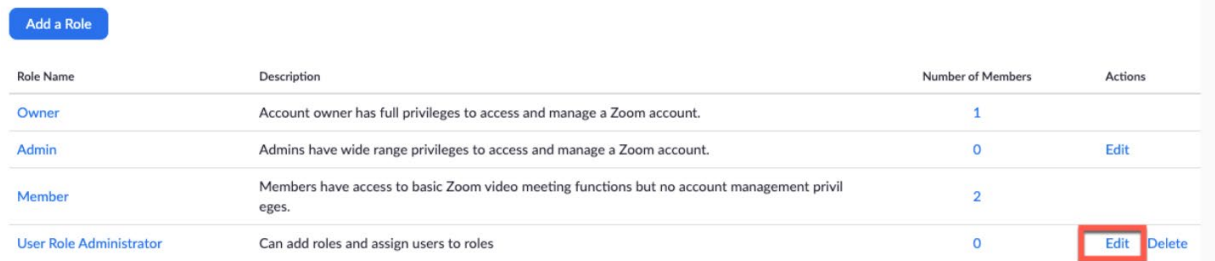
3.2 In what policy/procedure are the access controls identified in 3.1, documented?

,

<https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf>

The following screen shot lists the process of how to add/provision roles/privileges:

Each user will belong to one of the roles below, and different roles have their unique privilege.



Role Name	Description	Number of Members	Actions
Owner	Account owner has full privileges to access and manage a Zoom account.	1	
Admin	Admins have wide range privileges to access and manage a Zoom account.	0	Edit
Member	Members have access to basic Zoom video meeting functions but no account management privileges.	2	
User Role Administrator	Can add roles and assign users to roles	0	Edit Delete

3.3 Are there other components with assigned roles and responsibilities within the system?

No. There are no other assigned roles and responsibilities with ZoomGov outside of the roles provided in section 3.1.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

External parties will not have access to the ZOOMGOV system data. This includes an outside agency or external companies/contractors.

All appropriate FAR clauses such as CFR 24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act, have been incorporated into the contract and provide a foundation for the contractor's privacy data protection policies.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

ZoomGov retains data in accordance to EPA Records Schedule 1012 – Information and Technology Management. by retaining server logs for at least 12 months within their Splunk component and keeping records readily available online for 90 days.

Account owners can change the privilege to edit recordings using role management. If an account owner enables the privilege to edit recordings, the associated users can edit users' cloud recordings including the ability to disable the auto delete setting. There isn't a privilege for specifically disabling the auto delete setting.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

There's a small risk that data is retained longer than required.

Mitigation:

Account owners and administrators can delete discretionary content such as cloud recordings and chat logs (text messages, photos, and files). Once an account owner or administrator deletes this content it cannot be retrieved. We have also lowered this risk by limiting the sensitivity of recorded information. Record control schedule is regularly reviewed.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is

accessed and how it is to be used, and any agreements that apply.

No. Information is not shared outside of EPA as part of the normal agency operations for ZoomGov.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

There is no external sharing .

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

ZoomGov does not have any MOUs or Information Sharing Agreements (ISAs). No information is shared externally outside of EPA but if there becomes a need to establish new information sharing agreements, they will be managed in accordance with EPA procedures.

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable, there are no agreements.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

There is no risk related to information sharing since there no information shared outside the agency, therefore there no risk is incurred.

Mitigation:

None.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

EPA ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behaviour, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All EPA systems employ auditing measures and technical safeguards to prevent the misuse of data.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The US EPA implements a Rules of Behaviour (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the EPA implementation of User Information Security and Privacy Awareness Training (ISPAT) which is provided annually. In addition, all EPA personnel receive annual refresher cybersecurity training to educate them regarding the use and management of sensitive data.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of improper audit. There's a risk that the required information privacy controls may not be fully implemented or implemented properly.

Mitigation:

Privacy controls will be assessed prior to receiving an authority-to-operate (ATO) and as part of the NIST Risk Management Framework (RMF), continuous monitoring and annual security assessment will be conducted to ensure compliance with all privacy requirements.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

Information is collected and an approved ZoomGov administrator will enter that data to initially established an account for an EPA user. This process will provision a EPA license to a EPA user. Only users that have requested and have been approved for use of ZoomGov will be entered into the ZoomGov system.

Once a user is provisioned and setup with a ZoomGov account, the individual will enter information as needed to schedule and conduct ZoomGov meetings.

All information used and collected is kept to a minimum and only for the purposes of inviting ZoomGov users to a meeting.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes ___ No X. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)*

Authorized ZoomGov users typically retrieve information on the by activity type or activity title.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

There are no current systems of records for ZoomGov, however, a review of the system data has been fully identified and evaluated to determine the potential effect on the privacy of individuals.

ZoomGov has physical, technical and administrative controls in place to protect privacy and to limit access. The ZoomGov application is hosted in a FedRAMP cloud-based infrastructure hosted within AWS (Amazon Web Services) in the US. The physical security capabilities of AWS data center meet or exceed the EPA capabilities. ZoomGov protects data in transit via TLS 1.2 using 256-bit Advanced Encryption Standard (AES-256). Administrative controls such as requiring role-based training, signing Rules of Behavior (RoB) and restricting access to very small limited number of approved ZoomGov users and administrators and ZoomGov licenses.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is a low risk of inappropriate use or handling of the information necessary to establish or attend ZoomGov meetings.

Mitigation:

All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All EPA systems employ auditing measures and technical safeguards to prevent the misuse of data.

ZoomGov users and administrators are required to sign EPA Rules of Behavior (RoB). If inappropriate use or handling of information is suspected, ZoomGov account owners and authorized ZoomGov users are required to immediately report it to EPA CSIRC within 1-hour of discovery in accordance with EPA policy and established procedures.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Mitigation: