Federal Trade Commission
Privacy Impact Assessment

Table of Contents

1 System Overview 1

2 Data Type, Sources, and Use 1

3 Data Access and Sharing 4

4 Notice and Consent 7

5 Data Accuracy and Security 9

6 Data Retention and Disposal 10

7 Website Privacy Evaluation 10

8 Privacy Risks and Evaluation 10

1 System Overview

1.1 Describe the project/system and its purpose.

Zoom for Government (ZoomGov) is a web-based tool that allows video, voice, content sharing, and chat services and is used [1</MCID 3s>>BD7C hBT 4 0>>mBDC 00w8t (

to facilitate a seamless participant meeting experience and help ensure the participant's desired configurations are utilized in the meeting experience.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.

☒ Full Name
☐ Date of Birth
☐ Home Address
☒ Phone Number(s)
☐ Place of Birth
☐ Age
☐ Race/ethnicity
☒ Alias
☐ Sex
☒ Email Address
☐ Work Address
☐ Taxpayer ID
☐ Credit Card Number
☐ Facsimile Number
☐ Medical Information
☐ Education Records
☐ Social Security Number
☐ Mother's Maiden Name

☐ Biometric Identifiers (e.g., fingerprint, voiceprint)
☒ Audio Recordings
☒ Photographic Identifiers (e.g., image, x-ray, video)
☐ Certificates (e.g., birth, death, marriage, etc.)
☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)
☐ Vehicle Identifiers (e.g., license plates)
☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)
☐ Geolocation Information
☐ Passport Number

☒ UserID (First/Last Name)
☐ Internet Cookie Containing PII
☐ Employment Status, History, or Information
☐ Employee Identification Number (EIN)
☐ Salary
☐ Military Status/Records/ ID Number
☒ IP/MAC Address
☐ Investigation Report or Database
☐ Driver's License/State ID Number(or foreign country equivalent)
☒ Other(Please Specify): Open chat field where participants can enter any kind of information; recorded content, documents/files shared that may contain PII, language preference

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The FTC has configured ZoomGov to allow users to share various files for presentations and dissemination to other meeting participants. These files can be downloaded locally by meeting participants and/or featured in any recording. Such files can contain any and all types of information that may be nonpublic and sensitive in nature.

In addition to the PII elements identified in section 2.1 above, ZoomGov logs various non-PII elements (some of which may be connected to individuals' names or accounts) relating to events and usage for the meeting (e.g, total meeting time, date, start time, end time, topic, meeting ID, session ID, other metrics about when and how meetings were conducted, and what features were used), the device, end point and system environment attributes participating in the meeting (e.g. UUID, IP address, MAC address, operating system, user agent, average bandwidth), 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 or metadata.

2.3 What is the purpose for collection of the information listed above?

ZoomGov collects and stores participants' email addresses and names (including phone numbers and profile photo if provided). Email addresses, names, User IDs/aliases, as well as video images of users and profile pictures are used by Zoom to facilitate event access, authentication, performance, and event management. Email addresses can be used by the FTC to transmit ZoomGov invitations to recipients. When individuals are invited to a ZoomGov session via an email, they receive an email invitation from the event/meeting organizer with the details of the meeting, including the date, time, and any other relevant data. The link to join that particular session is embedded within the email invitation. A unique password is also included in the email invitation. The participant accesses the ZoomGov session by clicking on the embedded link in the email. Zoom stores the phone number of the billing point of contact and any phone numbers entered voluntarily into the profile information by a user as an optional field. This information is stored to enable that user to display their phone number to their contacts. A phone number will also be collected if Zoom Phone is used.

Provided that they have received prior authorization from an FTC account administrator, FTC meeting hosts or co-hosts may have the ability to record portions or entire ZoomGov sessions. This includes video, audio, as well as any public chat content generated during that particular session. Individuals will be notified if a meeting is being recorded and have the opportunity to leave the meeting or to mute audio and/or video to avoid having their voice and/or likeness recorded. The FTC can enable meeting hosts to record content for reference. Content can be stored both locally and in the ZoomGov cloud. The FTC has configured ZoomGov to allow users to share various files for presentations and dissemination to other meeting participants. These files can be downloaded locally by meeting participants and/or featured in any recordings for reference.

In addition to the PII elements identified above, ZoomGov logs various non-PII elements, as discussed above, for troubleshooting, security, operation and improvement of ZoomGov products and services, and performance improvement.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	Type of Data Provided & How It Is Collected
FTC staff/contractors (internal users)	FTC users must provide their email address in order to receive meeting invitations sent via ZoomGov. Names, photos and/or aliases are also collected when users log on to participate in a ZoomGov session. Depending on their participation, FTC users also contribute video and audio, text or file content to the ZoomGov session.

Source of Data	Type of Data Provided & How It Is Collected
Members of the public (external users)	Non-FTC users are also required to provide an email addr in order to receive a ZoomGov meeting invitation. When logging onto the ZoomGov session, individuals can opt to use their real names or choose usernames/aliases. The following information may also be collected by the FTC depending on the nature of the session: organization/company name; phone number; individual's photo and/or real-time video, real-time audio; chat messages and/or files.
Participants' Devices (of internal and external users)	ZoomGov collects information through metadata and operational 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 utilized in the meeting experience.
Zoom Meeting Sessions	ZoomGov generates and/or collects information relating to events and usage for meetings (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 related to meeting sessions.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	How and Why the Data Will Be Accessed/Shared
FTC staff/contractors (internal users)	Internal participants in ZoomGov meetings hosted by the FTC will be able to access or view the email addresses, participant names and photos of meeting participants (if provided), and the meeting name, description and login details for the session. In addition, internal participants will be able to see and hear real-time video and audio feeds for all participants in the session (if not muted or disabled by those participants), any photos participants have added to their Zoom backgroun

Data Will Be Accessed By and/or Provided To:	How and Why the Data Will Be Accessed/Shared
	and the contents of any chats or files shared with all participants during the meeting. The categories of information about live and past meetings and webinars hosted on the ZoomGov account that FTC designated administrators can access include: - Meeting information, including meeting ID, meeting topic, host name, start time, number of participants, whether participants join by phone, whether participants join audio via computer or mobile device, whether participants join with video, whether there was screen sharing during the meeting, whether the meeting is or was being recorded, whether an H.323/SIP device joined the meeting, whether the meeting is or was encrypted. - Meeting and participant profile information, including participant names; device participant was connecting from; IP addresses; location; network type (wired, wifi, 4G, etc.); network health (whether any warning level or critical level issues in meeting); issues (connection/client health warnings, e.g., unstable audio or video); selected microphone, speaker, and camera devices; which data center the participan connected to for the meeting; connection type (the data protocol type the participant is or was using); and join and leave times. - Detailed stats for Audio, Video, and Screen Sharing, including the bitrate, latency, jitter, as well as packet loss average and maximum. For Video and Screen Sharing, you can also view the resolution and framerate. - CPU Usage including the minimum, average, and maximum used by Zoom during the meeting/webinar, as well as the maximum used by a participant’s system (device) overall during the meeting. FTC Hosts and Administrators: in order to invite participants to hosted meeting using the individual's name/email listed in the system, the FTC Host must be a member of a built in group to create/invite meetings. FTC Administrators create, manage, and monitor internal FTC user accounts.

ZoomGov and Zoom Cloud Service Providers also may have system data access. See section 3.1 above. The ZoomGov cloud is hosted by AWS a dedicated cloud that is maintained separate from Zoom's commercial cloud. Zoom staff are subject to mandatory security awareness and privacy training for all users; role-based training for privileged users; personnel screening as required by FTC; and completion of contractual agreements and Rules of Behavior in accordance with applicable FTC policies. AWS also uses various security and privacy features to ensure protection, including as described by materials made available by AWS.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

FTC contractors are subject to the same FTC privacy incident response plan as its federal staff. Zoom maintains its own incident response plan and requires all employees to complete annual privacy and security awareness training.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (check all that apply):

- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (explain): Prior to joining a live session, participants are provided with a notice that information may be collected for US Government0o 395.4 cm 0..8 (f)-3.9 (1. [8[(o)e)1.9 (m)-

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

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Yes. When participating in a ZoomGov session, individual users have access to and can modify their user name, alias, contact information, and organization name. They also have the option to disable their camera and microphone features if they do not wish to make their picture or voice available to the rest of the participants.

Individuals may request access to federal agency records or information through Freedom of Information Act (FOIA) requests (with the exception of certain types of records). The Privacy Act allows most individuals to seek access to federal agency records about themselves and affords that person the right to challenge the accuracy of the information contained about them. An individual may make a request under the Privacy Act for access to information maintained and retrieved according to personal identifier by the FTC about themselves in the FTC's Privacy Act systems. The FTC's Privacy Policy provides links to the FTC's System of Records Notices (SORNs), as well as information about making Freedom of Information Act (FOIA) requests and the online FOIA request form. Individuals seeking access must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations (C.F.R.) at 16 C.F.R. 4.13.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Yes, see Section 4.3. In addition, to the extent the Privacy Act applies, the FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the FTC in agency records retrieved by the name of the individual or other p2w [(.)1torecor (a)veTawJ 3 Tr 27

or6.96priTd2 (o (10 (e)4 (d i)-2 (ndi)-2 (vi)y t)-2 -10 (r)3 (d)J 3 Tr p2w [(-2 (hxe)-10 (a)4 p (

w

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

On a quarterly basis, FTC ZoomGov System Administrators review the FTC configuration of ZoomGov to ensure the following: review account access; enabling, modifying, disabling and removing account access; and ensuring that only identified and registered assigned FTC personnel have access to the FTC Zoom instance.

5.2 Are there administrative procedures and technical sa (n)-8weg (n)-uatun p86 (s)-5(ccu)-81 (o)-4

- Zero

Risk	Mitigation Strategy
Unauthorized participants in ZoomGov meetings	Each Zoom session has a unique link, and a passcode ca added for additional security. Furthermore, the meeting host can create a “waiting room” for participants, where invitees must wait until the meeting host allows them to join the session. If an unauthorized individual attempts to join, the host can deny that individual from entering the sessions.
Third party access to FTC data	Both Zoom and its CSP (AWS) have access to FTC data collected and maintained through use of the system. Zoom employs role-based access controls, and data in the AWS cloud is encrypted and may not be accessed without prior consent from Zoom.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

ZoomGov contains a number of embedded privacy controls and enhanced functions designed to support privacy. These features incorporate privacy by design concepts such as the use of passcodes, the Waiting Room (host must admit participants individually), “only authenticated users can join meetings,” or blocking entry to users from certain countries/regions (to control which participants can join and have access to real time meeting content). Additional features include a list of all participants present in the meeting (to ensure transparency about who has access to real time meeting content); interruptive signals indicating that the meeting will be recorded; ability to mute audio, video and to use an alias; controls that prevent anyone other than the meeting host from recording the meeting using the built-in recording feature (unless the meeting host adds a co-host); and controls that allow the meeting host to lock the meeting and prevent additional participants from joining.

Recorded content that the meeting host does not store locally will be stored in encrypted storage in the ZoomGov cloud (a separate FedRAMP-authorized cloud distinct from commercial cloud), and will be accessible to FTC account administrators and Zoom support engineers if requested by the FTC. FTC account administrators can also choose whether cloud recordings can be shared publicly or internal-only—if at all—and otherwise select settings to limit access to the recording files. Users can only view their cloud recordings or any cloud recordings that have been shared with the specific user.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal investigatory files) subject to the Privacy Act. See the FTC's list of Privacy Act systems for more information, linked to the FTC's privacy policy, at www.ftc.gov/privacy.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The administrative and technical controls described in section 5.2 of this document provide assurance that the collection, use, and maintenance of the information will be conducted as described in this PIA. This PIA aligns with the FTC's existing privacy policies and procedures.