Federal Trade Commission
Privacy Impact Assessment

Zoom for Government (ZoomGov)

March 2021

Table of Contents

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 service and is used by the Federal Trade Commission (FTC) to collaborate in a virtual environment. The FTC's implementation of ZoomGov as a Software as a Service (SaaS) platform allows users to meet online, with or without video, and unifies cloud video conferencing, 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 (OS).

ZoomGov is used by the FTC to conduct virtual meetings both internally within the agency and externally with non-FTC entities. This includes members of the public, such as individuals that staff or represent other government agencies (local, state, and federal), members of Congress and/or their staff, external law enforcement partners and associations, industry representatives, consumer advocacy groups, etc.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The information in this system is collected, maintained and disseminated pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58. Information collected, generated, or maintained by the system for administrative and security purposes is authorized under the Federal Information Security Modernization Act (FISMA), Pub. L. No. 113-283, 44 U.S.C. 3551 et seq.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

In order to use ZoomGov, participants are required to provide an email address and user name; the user name could be the individual's real name or an alias. Additional information may also be collected depending on the nature of the session; this may include the person's company/organization name, phone number, photo, and/or real-time video (with user's permission). Information provided by participants to any meeting hosted by the FTC are used by the agency to allow participation in ZoomGov sessions; the FTC may also use some aggregate information for statistical purposes when assessing account usage and scope. Additionally, ZoomGov uses information about the types of devices and systems used by participants (e.g., computer type, speaker, microphone, operating system, average bandwidth)

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

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

☒ User ID (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 emailed 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 address 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 background,

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 participant 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.
Members of the public (external users)	Non-FTC individuals who use ZoomGov to participate in virtual meetings with the FTC will have access to the email

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
	addresses, participant names and photos (if provided) of other participants to the meeting, as well as the meeting name, description and login details for the session. In addition, external 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 background, and the contents of any chats or files shared during the meeting.
ZoomGov and Zoom Cloud Service Providers (CSPs)	Zoom engineers: Designated Zoom engineers can access data associated with FTC's ZoomGov account and sessions hosted on that account to provide the ZoomGov service to the FTC, including performance, authentication and event management and improvement. Zoom has access to participants' names/aliases, email address, what type of device the participant is using, and IP address. Amazon Web Services (AWS): As a CSP, AWS provides the hosted environment for ZoomGov and has access to FTC information that is encrypted at disk level for maintenance and technical support purposes.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes, authorized FTC contractors have access to FTC data in ZoomGov. FTC contractors are subject to the same rules and guidelines as FTC federal employees and must adhere to established FTC policies and procedures. FTC contractors are required to complete the mandatory Privacy and Security Awareness training upon hire and at least annually thereafter. FTC's use of Zoom for Government leverages the built-in groups for managing the different levels of access allowed upon the system. The FTC defined User Groups within the Zoom for Government system are the following: Administrators and Standard Users. These groups are required to obtain access authorization from the FTC Zoom system stewards before being granted access. Roles within the Zoom for Government application are assigned based upon Role Based Access Controls (RBAC) and the least privilege model. The assignments correspond to the performance of their required duties which are defined to be either Users or Administrators.

ZoomGov and Zoom Cloud Service Providers also may have system data access. See section 3.1 above. The ZoomGov cloud is hosted by AWS in 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 Government-authorized use. Communication or data transiting or stored by the FTC or on behalf of the FTC may be disclosed or used for lawful Government purposes as necessary.

☐ Notice is not provided (explain): ________________________________

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Yes. Individuals are required to provide their email address in order to receive the ZoomGov invitation. If they choose to not provide this information, they will be ineligible to participate in the session via ZoomGov. In addition, individuals can decline a meeting invitation and choose not to join a session hosted on ZoomGov or can disable video or audio during the session to prevent transmission of their voice or image; they may also choose to use an alias versus a real name during the meeting. 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. 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.

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 personally assigned identifier. See section 8.4 below. The FTC's Privacy Policy provides links to the FTC's SORNs, which include information about how to correct or amend records. An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in Privacy Act systems. Access to the information under the Privacy Act is subject to certain exemptions. Individuals may also file FOIA requests for agency records about them (if they are not exempt from disclosure to them under those laws). Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly.

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 FTC assigned personnel have access to the FTC Zoom instance**.**

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

PII is secured within the system maintained by the FTC through the use of administrative controls in the form of mandatory security awareness and privacy training for all users; role-based training for privileged users; personnel screening as required by the FTC; and completion of contractual agreements and Rules of Behavior, in accordance with applicable FTC policies. These controls include, but are not limited to, minimizing privileged users, prohibiting account sharing, and conducting monthly user audits.

Zoom utilizes administrative controls in the form of role-based access restrictions; mandatory security awareness and privacy training for all Zoom employees; personnel screening, including role-specific screening criteria; completion of contractual agreements and a Code of Business Conduct and Ethics; a formal sanctions process for those Zoom personnel who fail to comply with Zoom policies and procedures; a vendor selection committee process; and a Vendor Security Management Policy.

Physical controls include hosting applicable data within data centers (AWS) which control and monitor physical access to the system components, including visitor control and auditing of access records; and, protection of power equipment and cabling, transmission medium, output devices and use of emergency power and shutoff systems as well as fire and water damage protection.

Zoom employs Network Access Controls (NAC) and network monitoring to prevent unauthorized devices from physically connecting to the data centers/co-locations. Zoom employs next-generation firewall on both the production and corporate network, which includes advanced threat protection, which provides:

- Full visibility into all network traffic, including stealthy attempts to evade detection, such as the use of non-standard ports or SSL encryption.
- Attack surface reduction with positive security controls to proactively take away infection vectors.
- Automatic known threat prevention firewall, threat prevention, URL filtering, advanced endpoint protection and a security service, providing defenses against known exploits, malware, malicious URLs and command-and-control (C2) activity.
- Zero-day threat detection and prevention, including threat analytics with high relevance and context.

Zoom's administrative and technical controls are evaluated as part of the annual FedRAMP certification.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

GRS 3.1 covers General Technology Management records and GRS 3.2 for System Security Management records. The FTC will retain the recorded content and chats until such time that a NARA-approved records disposition schedule can be implemented.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Zoom employs cookies to recognize a device or user for purposes of performance, troubleshooting, authentication, anti-fraud and security. For additional information, see Zoom's Cookie policy.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes.	System administrators strictly manage access control and limit the use and access of all data to purposes for which it was collected. A system log is maintained that reflects who accessed the data at any given time, and whether the data was tampered with or edited.
Unauthorized participants in ZoomGov meetings	Each Zoom session has a unique link, and a passcode can be 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.

Risk	*Mitigation Strategy*
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 own 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 Register for this system/project? If so, list the applicable SORN(s).

Not applicable. ZoomGov is not considered to be a Privacy Act System of Records. The agency does not use Zoom to collect or maintain agency records retrieved by name or personally assigned identifiers. Information, including PII, communicated by or exchanged between FTC users and/or outside individuals, may be incorporated into agency records (e.g., 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.