United States Department of Agriculture

Office of the Secretary

Office of the Chief Information Officer

1400 Independence Avenue S.W.

Washington, DC 20250

SUBJECT: Zoom Usage at USDA

1. Purpose

This memo provides general user information about Zoom. It details what Zoom is, its capabilities, how it can be acquired, highlights security concerns, and how to use Zoom securely.

2. What is Zoom? An Overview of Capabilities

There are two versions of Zoom: Zoom Commercial and Zoom for Government. Zoom for Government platform unifies cloud video conferencing, simple online meetings, and a software-defined conference room solution into one easy-to-use platform. The solution supports Android, Blackberry, Zoom Rooms, and H.323/SIP room systems.

Zoom for Government Products includes the following services:

- **Zoom Cloud Video Conferencing.**—A cloud-based collaboration service which includes video, audio, content sharing, chat, webinar, cloud recording and collaboration.
- **Zoom Rooms.**—Software-based group video conferencing for conference and huddle rooms that run off-the-shelf hardware including a dedicated MAC or PC, camera, and speaker with an iPad controller.
- **Zoom API**.—Provides the ability for developers to easily add Video, Voice and Screen Sharing to your application. This API is a server-side implementation designed around Representational State Transfer (REST). The Zoom API helps manage the pre-meeting experience such as creating, editing and deleting resources like users, meetings and webinars.
- **Zoom Room**.—A stand-alone product. Zoom products also include the ability for audio dial-in with local numbers from around the world, wireless presentation, content co-annotation, webinars, and more.

3. Minimum Requirements for the Use of Zoom at the USDA

Please take note that these are the minimum requirements for the use of Zoom for official purposes. Some of these requirements are taken up in more detail in the "how-to" sections that follow.

- Zoom for Government is the only option authorized for use in the USDA—Commercial Zoom is not authorized
- Users are required to password protect all meetings in accordance with the USDA Authority to Operate
- Do not input or share any PII data when using Zoom
- Meeting invitees need to be controlled and distributed to only those identified as meeting participants.
- Users will implement the Waiting Room Feature for all meetings.

- ATO: Zoom for Government has a USDA wide ATO and is approved for use within the USDA.

4. Essential Tips for Using Zoom Securely

a. Generating Meeting ID and Password for Attendees

To host a meeting, individuals require a meeting ID and password. As a host, generate a random meeting ID when scheduling your event and require a password to join. Then you can share that meeting ID securely.

Zoom recommends you take every precaution in protecting your data when you are on the Internet. For example, change your passwords often, use a combination of upper and lower-case letters, numbers, and symbols when creating passwords, and make sure you use a secure browser.

To learn about meeting IDs and how to generate a random meeting ID, see this video tutorial (at the 0:27 mark) or go to https://youtu.be/XhZW3iyXV9U.

b. Password Protect Meeting for Security

Meetings and webinars can require passwords for an added layer of security. Passwords can be set at the individual meeting level or can be enabled at the user, group, or account level for all meetings and webinars.

Account owners and admins can also lock password settings, to require passwords for all meetings and webinars on their account. For additional information on passwords, see here or go to https://support.zoom.us/hc/en-us/articles/360033559832-Meeting-and-Webinar-Passwords-

c. How to Avoid Unwanted Guests/Participants

There are at least three ways to avoid unwanted guests:

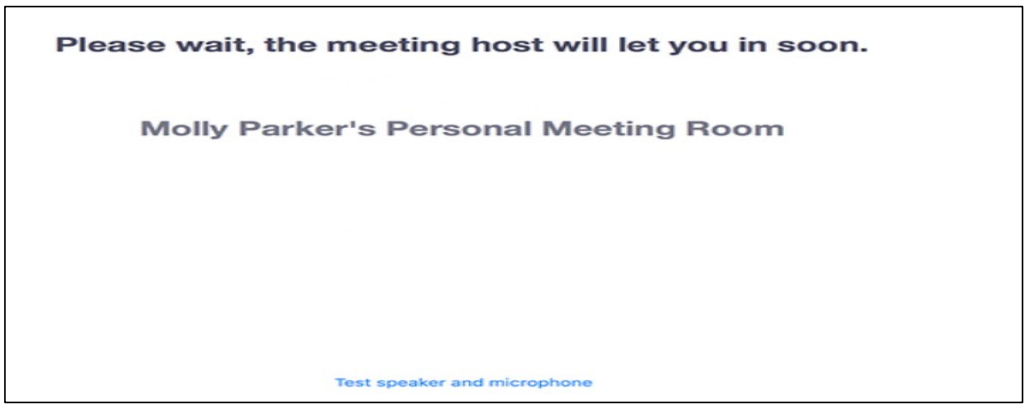
- Only send meeting invites to those expected to attend meeting.—Whenever possible, distribute your Zoom meeting link only to those individuals who will be attending your meeting.
- Do not distribute meeting invitation on social media.—If you share your meeting link on social media or other public platforms, anyone who sees the link will be able to join your meeting (unless you set a password for your meeting and share that privately with attendees). That includes trolls, who can then share or post inappropriate or offensive material ("zoombombing").
- Use the waiting room feature (see next section).

d. Use Waiting Room Feature to Manage Attendance

The Waiting Room feature allows the host to control when a participant joins the meeting. As the meeting host, you can admit attendees one by one or hold all attendees in the waiting room and admit them all at once.

You can send all participants to the waiting room when joining your meeting or only guests/participants who are not on your Zoom account or are not signed in.

Participants will see the following screen when joining a meeting with Waiting Room enabled:



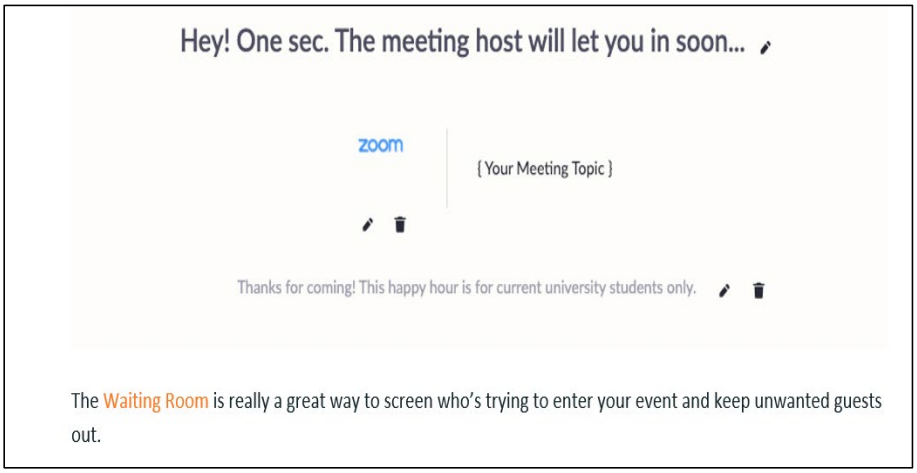
To use Waiting Room, the following system specifications apply to the Zoom Desktop Client:

- Windows: 4.6.2 or higher;
- macOS: 4.6.2 or higher;
- Linux 2.0.871.0317 or higher

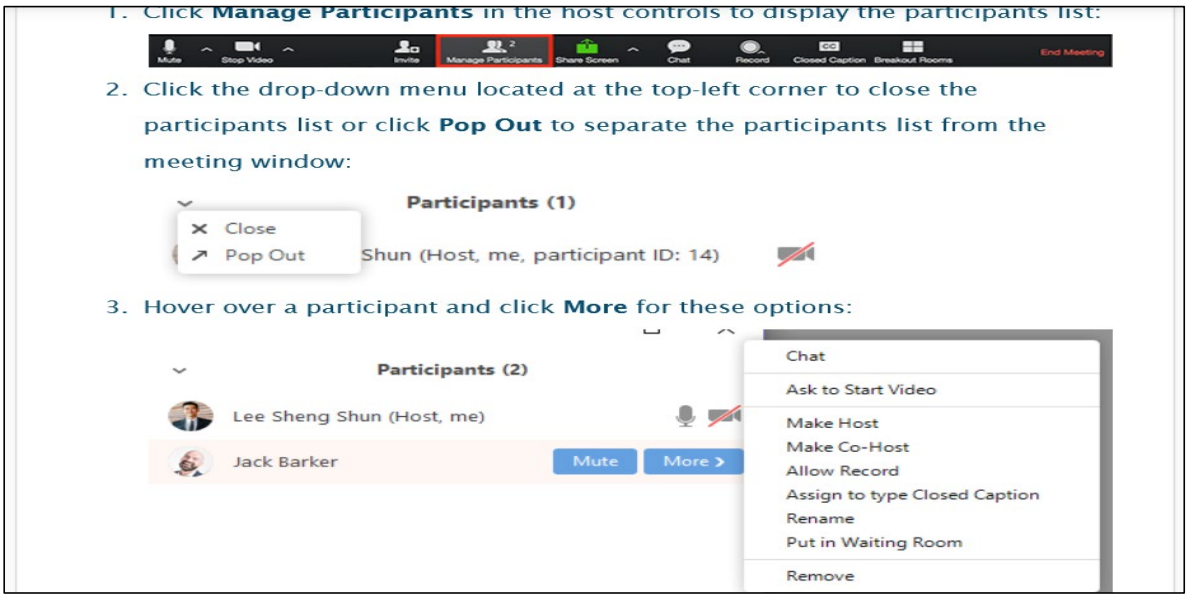
For more information on the Waiting Room feature, see here or go to https://support.zoom.us/hc/en-us/articles/115000332726-Waiting-Room

e. How to Set Up Waiting Room Feature

Meeting hosts can customize Waiting Room settings for additional control, and you can even personalize the message people see when they enter the Waiting Room so they know they're in the right spot. This message is really a great spot to post any rules/guidelines for your event, like who it's intended for.



From the Manage Participants menu, you can mouse over a participant's name, and several options will appear, including Remove. Click that to kick someone out of the meeting.



f. Protect Your PII! Never Share PII or Other Sensitive Information

Zoom does not require, process, store, or transmit PII. Users should nevertheless be careful not to expose PII on the platform.

Zoom uses a combination of industry-standard security technologies, procedures, and organizational controls and measures to protect your data from unauthorized access, use, or disclosure.

g. Using Zoom to Host Public Events

Zoom can be used to host public events.

- When you share your meeting link on social media or other public forums, that makes your event public. ANYONE with the link can join your meeting.
- Avoid using your Personal Meeting ID (PMI) to host public events. Your PMI is one continuous meeting and you don't want random crashing of your personal virtual space after the event is over. For information on Zoom PMI, click the link above or go to https://support.zoom.us/hc/en-us/articles/203276937-Using-Personal-Meeting-ID-PMI-

To learn about meeting IDs and how to generate a random meeting ID, go to https://support.zoom.us/hc/en-us/articles/201362413-Scheduling-meetings or see the video tutorial at https://youtu.be/XhZW3iyXV9U at the 0:27 mark.

5. How to Acquire Zoom Services, Licensing and ATO

- Zoom for Government is accessible at:
  - Zoomgov.com
  - https://www.zoomgov.com/download

- Zoom for Government is an authorized FedRAMP Moderate level system. Zoom for Government has a USDA wide Authority to Operate and is approved for use within the USDA. A separate ATO is NOT required.
- If you plan to HOST a meeting using zoom, the FREE version has a limit of 40 minutes per meeting of 3 or more participants
    - You will need to purchase licenses to host longer meetings
    - Work with your agency on how to purchase license for your team
    - For more information on licenses see the FAQ on the Zoom Gov website (https://www.zoomgov.com/pricing)

6. Installation Zoom of Services

Any commercial version of Zoom needs to be removed and a ticket needs to be submitted to the CEC for installation. Elevated privileges (administrator) are required for installation if the client is downloaded locally.