Ohio | Department of Administrative Services

Mike DeWine, Governor
Jon Husted, Lt. Governor

Matt Damschroder, Director

Virtual Meeting Guidance for State Agencies, Boards, and Commissions

Approved Tools for Virtual Public/Open Meetings

- State employees and contractors should be using the State's approved collaboration tools – **Microsoft Skype for Business (Skype) and Teams**.
- Skype and Teams are the state standard and they both provide robust security controls. If your agency needs to make your event open to the public, Teams Live Events offers the best solution in that it can broadcast to up to 10,000 attendees. (Microsoft is potentially increasing this limit. Awaiting written confirmation from Microsoft.)
- A possible alternative is Webex (Cisco Event Manager). A contract to expand the number of users is still in progress.
- **Please note**: If retention of chat/meeting content is critical, Teams has the capability to do so.
  Microsoft Skype will be deprecated in 2021, so if you are getting started, please use Teams.

Tools Not Recommended for Virtual Public/Open Meetings: Due to security and privacy concerns, DAS OIT strongly recommends against using the following:

- **Zoom:** In recent weeks, Zoom has come under fire for its security and privacy practices. The Federal Bureau of Investigation (FBI) warned users of Zoom:
  - Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
  - Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
  - Manage screen sharing options. In Zoom, change screen sharing to "Host Only."
  - Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.
  - Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.
  - The FBI also warns that at least some Zoom servers are located in China.
  - FBI Guidance: https://www.us-cert.gov/ncas/current-activity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom
  - Additional Information: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a- quick-look-at-the-confidentiality-of-zoom-meetings/

  If a meeting is being held by an external party and is only offered via Zoom, it is acceptable to participate provided sensitive information is not shared or discussed.
- **Any free or non-business class tools**. These products are not properly vetted and could pose a risk to information security and privacy. Please do your own risk assessment and use it as appropriate.

Questions regarding the findings in this document or regarding the use of virtual public/open meeting tools can be directed to the DAS Office of Enterprise IT Architecture and Policy at DAS.State.IT.Standards.Manager@das.ohio.gov.