When to use Zoom?

1. The meeting has been set-up by an external vendor, agency, organization, or business
2. There is mandatory need to meet per continuity of operations of essential critical infrastructure during COVID-19
3. The outside organization cannot use a county-hosted WebEx or Teams teleconference platform
4. You are not sharing any confidential county information over the call

To discuss confidential county information, always utilize a WebEx or Teams meeting using a county platform.

If the sponsoring organization using Zoom is open to configuration recommendations, the following are noted by the FBI:

1. Zoom Meetings/classrooms are not public
2. Password required for meeting OR waiting room feature enabled to control admittance of guests
3. Do not share the link to a teleconference or classroom on a social media post; provide directly to specific people
4. Change screensharing to "Host Only"
5. Ensure all meeting attendees are using the most recent version of Zoom, since many security updates have been released between Jan-April 2020
6. Avoid zoom-bombing by turning off "join before host"
7. Turn off "allow removed participants to rejoin"
8. Turn off file transfer
9. Do not record the meeting, as there have been breaches of zoom recordings in the past

Other Zoom Platform Security Concerns (FYI)

Key security concerns related to Zoom that have not been addressed by the company include the following:

- There is no true end-to-end encryption; although the video is encrypted between two recipients, once it passes Zoom's firewall, it is unencrypted and available for Zoom to view. End-to-end encryption means that the video is hidden from Zoom employees and anyone who obtains the video.
- 5 of the 73 zoom key servers are located in Beijing, China, meaning that if the meeting were intercepted, they would be able to decrypt the contents
- AES security keys used to encrypt the video content between the client and zoom servers is only 128-bit using ECB encoding. ECP preserves pattern inputs (one of AES' worst encryption modes) and is easier to decrypt by a malicious actor.