Zoom Usage Guidelines

August 11, 2020

Introduction

In early 2020, Zoom's userbase expanded exponentially in response to increased demand for virtual collaboration tools caused by the COVID-19 pandemic. During this time, several major security issues were identified with the Zoom platform. In response to these issues and concerns, Zoom halted feature development and committed to an aggressive 90-day security improvement plan. This plan was initiated on April 1, 2020, and outlined seven commitments to secure and harden the platform, and to remediate the identified security and privacy issues.

Zoom recently completed this 90-day plan. In a July 1, 2020, message to customers, they outlined the status of the seven commitments made to improve the security and privacy protections of the Zoom application. Additionally, they outlined key leadership changes and additions, additional offers of Zoom for Government (hosted in Amazon Web Services Government Cloud), and additional U.S.-based product engineering teams to support the company's continued growth.

Based on the platform's new security stance, it is appropriate for the Texas Department of Information Resources (DIR) to update its previous Zoom usage guidance. This updated document provides suggestions and guidance on the use of Zoom and other virtual collaboration tools. As with any technology, organizations should always consult the most recent documentation from the technology platform developer. Each organization should thoroughly evaluate the use of each system against the security requirements of the organization.

DIR Usage Position

DIR has reviewed Zoom's progress on the implementation of their 90-day security plan. In coordination with the Texas Information Sharing and Analysis Organization, DIR has also conducted and reviewed additional third-party research and analysis on the Zoom platform. Based on the currently available evidence, DIR has concluded Zoom is now a viable candidate for online collaboration and is an acceptable platform for conducting state business involving both public and sensitive communications. DIR continues to strongly recommend against using Zoom for highly confidential conversations, meetings, or data transfer. Additionally, DIR recommends against using the recording feature for sensitive and confidential meetings. While it may be appropriate to host and record a public webinar or board meeting using Zoom, the risks of recording a sensitive internal meeting using the platform may be prohibitive.

DIR encourages all organizations currently using or considering the use of Zoom to explore Zoom for Government, which has been granted FedRAMP Moderate Authorization.

It should be noted that both the U.S. Department of Homeland Security (DHS) - Cybersecurity & Infrastructure Security Agency (CISA) and the U.S Department of Defense (DoD) have established guidelines for the authorized use of Zoom in their respective organizations. The guidance provided in this document aligns with these federal usage guidelines.

Security Points of Consideration for Agency Use

Zoom does not encrypt meeting traffic over its own internal network and servers. This practice is required to support the cloud-based recording of meetings and webinars, a key business function for Zoom. Session recordings are processed after the meeting and encrypted when stored. They can also be password protected or shared to members of your organization; however, during the recording process, the session is available on Zoom's infrastructure unencrypted. Should their systems be compromised, any live recording or open session would be exposed to the attack.

As meeting traffic is internally unencrypted, each organization should evaluate the risk of exposure for sensitive or confidential meeting traffic. DIR recommends against recording these meetings or sharing documents as attachments through the meeting platform.

Each organization must evaluate the use of any virtual collaboration platform against the security requirements of that organization. When in doubt, users should consult with their IT professionals and management to ensure the platform does not present an unacceptable risk to the organization. DIR reminds users to always follow their organization's policies addressing virtual meetings, information security, and records retention when using virtual collaboration tools.

DIR recommends users of all virtual collaboration platforms to become familiar with the meeting security settings and features to minimize potential disruptions during meetings and webinars. Additional details can be found in the next section.

General Virtual Collaboration Tool Configuration Recommendations

Virtual collaboration tools are feature-rich programs with many configurations that can support open collaboration or communication based on how the tool is configured. Below are general configuration recommendations to support security and reduce the chance of meeting disruption.

- Schedule meetings that require a password to join. Distribute passwords to attendees separately, via email.
- Turn on the "waiting room" feature to view and control which users are admitted into the meeting. Users can enable waiting rooms when scheduling the meeting or as a system-wide configuration.
- Lock meetings once all participants have joined. This will prevent unauthorized users from gaining entry while the meeting is in session.
- After locking the meeting, review the list of participants and expel any unknown participants before sharing your content.
- Expel disruptive individuals from your meeting.
- If supported by your system, disable the feature that allows participants who have been previously removed to rejoin.
- Disable participants' ability to record the meeting.
- Disable participant screen or file sharing. This will prevent your meeting from being disrupted by others and the sharing of inappropriate or potentially malicious content.
- Disable the chat feature prior to the start of the meeting.
- Put all attendees in mute mode and suspend privileges for participants to unmute themselves until needed.

- Avoid using personal meeting IDs for public-facing meetings.
- Consider publishing the meeting link via email to the desired attendees, rather than positing the link on public websites or calendars.
    - For public and other open meetings, such as board meetings, consider scheduling a webinar and requiring attendee registration.
- Avoid posting photos or screenshots of your meetings. This could provide threat actors with the associated meeting ID and information on who is attending your meetings.

Virtual collaboration tool administrators should carefully review their system, group, and user configurations and reach out to their vendors for support as needed. As with any technology, it is critical to update software and apply security patches on a regular basis. End users are encouraged to review the DIR Virtual Collaboration Tools Security Tips document for additional guidance.

Alternative Services Available

Multiple collaboration software services are available through DIR's Cooperative Contracts Program. A list of these cooperative contracts is available here: https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Cooperative%20Contracts%20for%20Remote%20Access.xlsx

DIR does not endorse the use of any specific product or solution. It is incumbent upon each organization to evaluate the use of any virtual collaboration platform against the security requirements of the organization.