MONTANA SITSD

SITSD NEWSBYTES

April 6, 2020

Online Meeting Security Recommendations

With remote work expanding across the United States in response to social distancing measures implemented to slow the spread of the novel coronavirus, many have turned to holding meetings via Internet-based communications platforms ("online meetings"), such as Zoom, Skype, Polycom RealPresence, and Teams.

On March 30, 2020, the FBI released an article warning users that teleconferencing sessions had been hijacked (also known as "Zoom-bombing") all over the nation. In several cases, the hijackers disrupted meetings by displaying obscene materials, hate images, and threats. The FBI has published the recommendations below, each of which is followed by additional suggestions from SITSD.

Montana's public participation requirements do not make distinctions based on meeting format. Therefore, agencies holding online meetings must ensure they comply with public meeting statutes, rules, and policies, just as they would when holding in-person meetings.

FBI Recommendations

- 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.
    - **SITSD suggests**: Prior to setting up a meeting, the organizer must first determine whether the online meeting is a meeting that must be open to the public pursuant to section 2-3-203, MCA. If a password will be required to attend a public meeting, the meeting organizer must ensure that the public has notice of the meeting and of the password requirement sufficiently in advance to allow members of the public to obtain a password from the meeting organizer before the meeting.
- 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.
    - **SITSD suggest**s: If the online meeting is a public meeting, the agency must provide notice of the meeting. The meeting organizer may use the meeting notice to share contact information that individuals interested in attending the meeting could use to obtain the meeting link and password.
- Manage screensharing options. In Zoom, change screensharing to "Host Only."

    - **SITSD suggests**: The presiding officer of a meeting should always be able to control the flow of the meeting, whether in-person or online. It is customary for meeting participants to seek recognition from the chair to ask questions, speak, or present. An online meeting is no different.
    - **SITSD suggests**: Depending on the circumstances and agency public participation rules, it may be necessary to allow the public to comment on matters discussed during the meeting. Sometimes the public's right to participate in a meeting may require offering an opportunity to share opinions, arguments, or materials prior to an agency decision. In such cases, the agency may require the materials to be submitted in advance. If the agency will consider materials that were not submitted in advance, the agency may collect the material via another channel (e.g. email, file transfer) during the meeting and redistribute. If necessary, the agency can recess to allow meeting participants to review the materials and reconvene to discuss them.
- 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.
    - **SITSD suggests**: Users should engage technical staff to ensure they are always using the correct product and version to conduct the meeting. SITSD recommends using Microsoft Teams for meetings consisting solely of state employees and contractors with an active directory account. Other products, including Zoom, may be used when meetings must be open to the public.
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

Additionally, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released a notice regarding this activity and added the following recommendations as this issue is not specific to Zoom, but rather applies to all video teleconferencing (VTC) software:

- Consider security requirements when selecting vendors. For example, if end-to-end encryption is necessary, does the vendor offer it?
- Ensure VTC software is up to date.
    - **SITSD suggests:** In addition to using the current version of the software or service, the meeting organizer should be familiar with the product's features and policies before setting up the meeting. The organizer can use this information to configure the product to allow the appropriate level of participation while minimizing the risk that the meeting can be hijacked.

The information below is provided by vendors regarding the privacy, security, and use of online meeting software and services that are commonly used by Montana state agencies.

- Zoom Privacy
- Zoom Management of User

- Zoom Message to Users
- Zoom Encryption
- Prevent “Zoom Bombing”

Security Tips for Common Virtual Collaboration Tools

GoTo Meeting

- Use the “Attendee List” pane to view all meeting attendees, change their presenter rights, or revoke attendee privileges.
- When sharing content select “Show Only” to share the desired information from your computer. This selection will show an animated gray frame indicating what attendees will see if selected.
- Require attendees who join via telephone to enter their Audio PIN. This gives the organizer audio controls for each participant. If users did not enter their audio PIN, right-click the person's name and select “Send Audio PIN”.

Teams/Skype

- Use the “Chat Pinning” tool to ensure you are chatting with the correct recipients.
- Understand that chat, channel, and files data are retained forever unless the system admin has actively modified retention policies.
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads.
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile.

Zoom

- Make meetings “Private” by requiring a strong meeting password.
- Select the “Enable Waiting Room” option to control the admittance of guests.
- Before a meeting begins, set screen sharing to “Host Only.”
- Check your workspace for unwanted objects, documents, or notes in view of attendees.
- Prevent unauthorized access by locking the meeting after all participants have joined. From the “Manage Participants” option click “Lock Meeting.”

WebEx

- Schedule “Unlisted” meetings and hide specific details, such as its host, topic, and starting time.
- Do not allow attendees to “Join Before Host.”
- Set up each meeting to require all attendees to enter a password. Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting.
- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone.