Michelle Lujan Grisham
New Mexico Governor

John L. Salazar
Cabinet Secretary Designate and State CIO

NM DEPARTMENT OF INFORMATION TECHNOLOGY
PROGRESS STARTS HERE

* * MEMORANDUM * *

TO: Department CIO and IT Leads
FROM: John L. Salazar, Cabinet Secretary Designate and State CIO
DATE: April 14, 2020
SUBJECT: On-line meeting product risks and security best practice guidelines

---

BACKGROUND INFORMATION:

As state employees are working remotely, safety, privacy and security of our staff members and state digital assets should be provided adequate protection and compliance maintained as per statues and best practices.

With state-sponsored remote meeting events increasing significantly, DoIT subject matter experts have created a set of recommendation and best practice guidelines for conducting remote state meetings using various software products. Additionally, DoIT is providing guidance on the use of online Collaboration Tools to address sharing of files in a secure environment.

While there are several products available on the market providing features for conducting online meetings and collaboration services, we are offering the following recommendations to bring consistency and risk-based guidance to mitigate potential dangers associated with the use of software products on the state's extended network and computing facilities.

The most popular software products on the market for conducting online meetings and collaboration services are the following:

1. Microsoft Teams
2. WebEx
3. Zoom

Details for each of the popular and widely used software products identified above, their functionality, DoIT recommendation for use of the product, pricing consideration and best practices are documented below:

1) **Microsoft Teams**: Microsoft (MS) Teams offers an organizational hub for instant messaging (chat) functionality, video meetings with the ability for screen/file sharing, file storage (including collaboration on files) along with other MS application integrations, OneNote, Word, Excel, Delve, Planner, etc. Within the MS Teams, you can have individual or group conversations, as well as, "Team" spaces with specific topics or users to communicate and collaborate. Team

spaces offer the ability to create specific channels (subject interest) within each "Team" space and each channel has chat as well as a file repository for documents shared within the "Team." Each channel also comes with a Wiki page to be used for documentation or meeting notes. MS Teams support up to 250 participants with the ability to add "guest" users for moderated access. MS Teams also offers the ability to host "Live events" that creates a protected, moderated stream event that can be locked down to active participants, viewer participants can ask questions in a moderated Q&A session as well as opening up a live stream to the public. MS Teams meets most security compliance standards such as CJIS & HIPAA.

DoIT Recommendations: *DoIT subject matter experts* ***recommend*** *agencies seriously consider utilizing the product because it provides both online meeting features and collaboration services.*

Pricing consideration: *MS Teams is included in O365 licenses and Microsoft is allowing free use of the service through September 31st, 2020.*

Best Practices Documentation - Exhibit A, *on page 4, is included in this document to provide best practices on the use of Microsoft Teams.*

2) **Cisco Webex Enterprise** –Cisco has **Meetings** functionality**.** The app supports 200 participants. **Event Center** allows up to 3000 contributors, in an online hosted forum that can be streamed to the public. Webex Enterprise also includes **Learning Center** for instructor lead meetings, **Support Center** for remote support services as well as **Webex Teams** for online collaboration. Cisco Webex integrates well with Microsoft Teams and licensing can be purchased via Named User and Knowledge User depending on which works best for each agency. Full HIPAA compliant and meets many additional compliance standards.

DoIT Recommendations: *DoIT subject matter experts* ***recommend*** *agencies seriously consider utilizing the product because it provides both online meeting features and collaboration services.*

Pricing consideration: *Cisco is allowing free use of the service through June 30th, 2020.*

Best Practices Documentation - Exhibit B, *on page 8, is included in this document to provide best practices on the use of WebEx.*

3) **Zoom**: This solution gained in popularity due to reliability and ease of use, unfortunately the ease of use also makes is susceptible to several security vulnerabilities. Recently, many are discussing the poor privacy and security practices surrounding ZOOM. Many companies are not allowing the use of the app. While DoIT **does not** currently recommend the use of this product, if Agencies choose to use the product, please refer to the best practices that are listed below as Exhibit C on page 11 to decrease the Agencies security liability.

DoIT Recommendations: *At this time, DoIT subject matter experts* ***don't recommend*** *the use of this product due to the widely reported security issues identified with the product.*

Pricing consideration: *Zoom offers a free service for up to 100 meeting participants.*

Best Practices Documentation - Exhibit C, *on page 11, is included in this document to provide best practices on the use of Zoom.*

ACTION RECOMMENDED:

The Department of Information Technology recommends state agencies use Microsoft Teams or Cisco Webex software products to conduct state sponsored online meetings. In the event the two products are not available, state agencies utilizing ZOOM should adhere to the ZOOM Best Practices listed on page 11.

For more information or additional details please reach out to our service desk at **505-827-2121** or EnterpriseSupportDesk@state.nm.us to be directed to the appropriate personnel.

Exhibit A - Best practices while using Microsoft Teams

Privacy and security in Microsoft Teams

As your team moves forward with video conferencing, we want to continue to provide the best practices for safety, privacy, and security. Please see this document directly from Microsoft describing the controls for Microsoft Teams:

From Microsoft: Over the past few weeks, there has been much written about video conferencing, privacy, and security. You may have questions and we want to help. Privacy and security are always top of mind for IT, but never more so than at this moment, when users are working remotely. Recently, Microsoft shared best practices for enabling remote work and security. This document outlines the security approach directly from Microsoft.

Privacy and security controls for video conferences in Teams

- **Meeting options**: With meeting options, you can decide who from outside of your organization can join your meetings directly, and who should wait in the lobby for someone to let them in. PSTN callers will be joining via lobby. Meeting organizers can also remove participants during the meeting.
- **Roles in a meeting**: A meeting organizer can define roles in a Teams meeting that designate "presenters" and "attendees," and control which meeting participants can present content in the meeting.
- **Attendee consent for recording**: All recordings of meetings are accompanied by a notice to attendees that a recording is taking place. The notice also links to the privacy notice for online participants, and the meeting organizer controls which attendees can record.
- **Meetings recording access**: Meeting recording access is limited to those people who are on the call, or invited to the meeting, unless the meeting organizer authorizes others to access the recording. Recordings are uploaded to Microsoft Stream and may be shared and downloaded according to permissions enabled by account administrators.
- **Channel moderation and controls**: Channel owners can moderate a channel conversation and control who is, and is not, allowed to share content in channel conversations. This helps ensure only appropriate content is viewed by others.
- **Communication compliance**: Communication compliance enables organizations to foster a culture of inclusion and safety by identifying and preventing negative behaviors like bullying and harassment.

Safeguard your privacy

When you use Teams, you are entrusting us with one of your most valuable assets—your data and personal information. Our approach to privacy is grounded in our commitment to giving you transparency over the collection, use, and distribution of your data. Far from an afterthought, privacy is deeply ingrained in our company philosophy and how we build products. Here are a few of our key privacy commitments to you.

- We never use your data to serve you ads.
- We do not track participant attention or multitasking in Teams meetings.
- Your data is deleted after the termination or expiration of your subscription.
- We take strong measures to ensure access to your data is restricted and carefully define requirements for responding to government requests for data.
- You can access your own customer data at any time and for any reason.
- We offer regular transparency reports on the Transparency Hub, detailing how we have responded to third-party requests for data.
- We have taken steps to ensure that there are no back doors and no direct or unfettered government access to your data.

Protect your identity and account information

- **Multi-factor authentication (MFA)**: Multi-factor authentication requires users to provide additional forms of verification to prove their identity, helping protect their accounts from attacks that take advantage of weak or stolen passwords.
- **Conditional Access**: Conditional Access allows you to set risk-based policies for access based on user context, device health, location, and more.
- **Microsoft Endpoint Manager**: Microsoft Endpoint Manager allows you to manage devices and apps and enforce Conditional Access on any device.
- **Secure guest access**: Secure guest access allows users to collaborate with individuals outside their organization while still controlling their access to organizational data.
- **External access**: External access provides an authenticated connection to another organization, enabling collaboration between organizations.

Protect your data and defend against cybersecurity threats

- **Encryption**: Teams data is **encrypted in transit and at rest**. Microsoft uses industry standard technologies such as TLS and SRTP to encrypt all data in transit between users' devices and Microsoft datacenters, and *between* Microsoft datacenters. This includes messages, files, meetings, and other content. Enterprise data is also encrypted at rest in Microsoft datacenters, in a way that allows organizations to decrypt content if needed, to meet their security and compliance obligations, such as eDiscovery.
- **Data Loss Prevention**: Data Loss Prevention prevents sensitive information from accidentally being shared with others.
- **Sensitivity labels**: Sensitivity labels allow you to regulate who can access a team by controlling the privacy and guest settings of the team.
- **Advanced Threat Protection**: Advanced Threat Protection helps protect users from malicious software hidden in files, including files stored in OneDrive or SharePoint.
- **Cloud App Security**: Cloud App Security provides you with tools to identify and mitigate suspicious or malicious activity, including the large-scale deletion of teams or addition of unauthorized users.

Meet more than 90 regulatory and industry standards

- **Compliance and regulatory standards**: To comply with global, national, regional, and industry-specific regulations, Teams supports more than 90 regulatory standards and laws, including HIPAA, GDPR, FedRAMP, SOC, and Family Educational Rights and Privacy Act (FERPA) for the security of students and children.
- **Information barriers**: Information barriers allow you to control communication between users and groups in Teams to protect business information in cases of conflict of interest or policy.
- **eDiscovery, legal hold, audit log, and content search**: eDiscovery and related features allow you to easily identify, hold, and manage information that may be relevant in legal cases.
- **Retention policies**: Retention policies allow you to manage content in the organization by deleting or preserving information to meet organizational policies, industry regulations, and legal requirements.

See Teams Technical Security Guide - link here for detail oriented information on all the security capabilities in Teams

Privacy and Security in Microsoft Teams created and maintained by Microsoft to ensuring privacy and security for Teams users, referenced above, can be found at the link here.

Best User Practices for Meetings

- Use **Microsoft Teams** for audio/video and web conference meetings. Invite attendees. Use the lobby feature for approved guests only.
- **Share your screen carefully** by managing options in your meeting.
- If **recording a meeting**, make sure everyone on the call is aware.
- **Do NOT** share a link to online meetings on unrestricted social media posts or platforms.
- **Do NOT** share confidential information in online meetings.

SETTING UP YOUR AUDIO, VIDEO AND ENVIRONMENT

Use a headset with mic if possible. This provides the optimal audio experience for both you and other meeting attendees. If a headset isn't available, use your device's built-in audio/mic. Call in via phone only as a last resort. **If you DO call in, make sure your computer/laptop's mic and speakers are muted.**
Avoid sitting with your back to a window or bright light source. This causes a silhouette appearance where others cannot see you or determine your identity.
Think about the background. Whatever is in the room behind you might not be appropriate for a meeting or could be distracting to others. Cameras pointed up at ceiling fans are also a visual distraction for some attendees. Consider using the *blur my background* feature in MS Teams. You can find this tool by clicking on the three dots when in a call.

Close doors to avoid unexpected visitors. Many are working in environment where other individuals (or other distractions) may pass by or inadvertently interrupt the meeting.

JOINING A MEETING

Join a few minutes early if possible. This allows you to make sure everything is working and gives time to make any adjustments.
Mute other devices and apps. Make sure to mute your cell phone, radios, televisions and close any other apps on your computer/laptop that might send distracting notifications.
Enter muted. Enter any meeting with your mic muted and camera off. Others might already be engaged in conversation.
Have a moderator or convener for large meetings. Consider appointing someone as convener or moderator for large meetings. This person can help bring forward any chat questions and provide meeting guidelines and reminders.

ATTENDING AND PARTICIPATING IN A MEETING

KEEP YOUR MIC MUTED. Most important: Keep your mic muted unless you need to speak or are leading the meeting. If your audio becomes distracting, others in the meeting may mute you. You will need to unmute yourself to begin speaking when needed. Those attending via call-in only will need to press *6 to unmute themselves if this occurs.
Avoid talking over others. Unlike an in-person meeting, its sometimes difficult to distinguish between multiple conversations leading to confusion.
Be clear, concise. Speak in a concise and clear manner and tone so that everyone can hear what you are saying.
Pause. Remember to pause occasionally to assure attendees have time to ask questions.
Camera use. Currently, up to four video feeds can be seen at any given time. (Microsoft is working to expand this feature). Video feeds automatically show or hide based on participation. Be sure to pause/turn off your camera if it may be distracting to others. Don't walk around with your camera on (mobile device).
Use chat window. Consider, especially for large meetings, asking your questions in the chat window.
Tag individuals in chat. Tag other attendees (using @userid format) in the chat window when your comment is directed towards a specific attendee to distinguish between a general comment.
Meeting recording. A participant can start a meeting recording. If recording a meeting is appropriate, announce that you will do so and confirm there is agreement. Meeting recordings become available shortly after the conclusion of the meeting on the Microsoft Stream services for members of the organization.

Exhibit B - Best practices while using WebEx

Securing Webex

- Cisco Webex Meetings provides a secure environment, yet it can be configured as an open place to collaborate. Understanding the security features as site administrators and end users can allow you to tailor your Webex site to your business needs.
- Additional Security details and information can be found in Webex Security White Paper.

Best Practices for Hosts

- As a host, you are the final decision maker concerning the security settings of your meeting. Always remember that you control nearly every aspect of the meeting, including when it begins and ends.
    - Do not share your Audio PIN with anyone
    - Provide meeting passwords only to users who need them.
    - Never share sensitive information in your meeting until you are certain who is in attendance.

Personal Room

- You set your Personal Room to automatically lock when your meeting starts. We recommend locking your room at **0 minutes**.

Consider using Personal Room Notifications Before and during a Meeting

- If you lock your Personal Room, you are able to screen anyone waiting in your lobby. After you enter your meeting, you are notified when someone new enters the lobby, and you can then choose whether to admit the person or not.
- Hosts can opt not to list the meeting on the meeting calendar to help prevent unauthorized access to the meeting and hide information about the meeting, such as its host, topic, and starting time.
- Choose a level of security based on the meeting's purpose. For example, if you schedule a meeting to discuss your company picnic, you can set only a password for the meeting. If you schedule a meeting in which you will discuss sensitive financial data, you may not want to list the meeting on the meeting calendar. You may also choose to restrict access to the meeting once all attendees have joined.

Choose the Meeting Topic Carefully

- A listed meeting or a forwarded invitation email could, at a minimum, reveal the meeting titles to unintended audiences. Meeting titles can unintentionally reveal private information, so ensure that titles are carefully worded to minimize exposure of sensitive data, such as company names or events.

Secure Meeting with Complex Password

- Using complex meeting passwords for every session is the most important step you can take to protect your meeting. While uncommon, site administrators may choose to allow the creation of meetings without passwords. Under most circumstances, protecting all meetings with a strong password is highly recommended.

Exclude Meeting Password from Invitations

- If you check **Exclude password from email invitation** when you schedule a meeting, the password will not appear in the invitation. You must provide the password to attendees by another means, such as by phone.

- For highly sensitive meetings, exclude the meeting password from the invitation email. This prevents unauthorized access to meeting details if the invitation email message is forwarded to an unintended recipient.

Require Attendees to Have an Account on Your Site

- When this setting is enabled, all attendees must have a user account on your site to attend the meeting. For information about how attendees can obtain a user account, ask your site administrator.

Use Entry or Exit Tone or Announce Name Feature

- Using this feature prevents someone from joining the audio portion of your meeting without your knowledge. This feature is enabled by default for Webex Meetings and Webex Training.

Restrict Available Features

- Limit the available features, such as chat and audio, if you allow attendees to join the meeting before the host.

Request That Invitations Are Not Forwarded

- Request that your invitees do not forward the invitation further, especially for confidential meetings.

Assign an Alternate Host

- Assign an alternate host to start and control the meeting. This practice keeps meetings more secure by eliminating the possibility that the host role is assigned to an unexpected, or unauthorized, attendee, in case you inadvertently lose your connection to the meeting.

Restrict Access to the Meeting

- Lock the meeting once all attendees have joined the meeting. This practice prevents more attendees from joining. Hosts can lock or unlock the meeting at any time while the session is in progress.

Validate Identity of All Users in a Call

- Accounting for every attendee by using a roll call is a secure practice. Ask users to turn on their video or state their name to confirm their identity.

Remove a Participant from the Meeting

- Participants can be expelled at any time during a meeting. Select the name of the participant whom you want to remove, then select **Participant** > **Expel**.

Share Application, Not Screen

- Use **Share** > **Application** > instead of **Share** > **My Screen** to share specific applications and prevent accidental exposure of sensitive information on your screen.

Assign Passwords to Recordings

- The best way to prevent unauthorized access to recordings is not to create recordings.

- If recordings must be created, you can edit meeting recordings and add passwords before sharing them to keep the information secure. Password-protected recordings require recipients to have the password in order to view them.

Delete Recordings

- Delete recordings after they are no longer relevant.

Personal Conferencing for Hosts

- Create a strong Audio PIN and protect it. On your Webex site, go to **My Webex Preferences** in Classic View, or go to **Preferences** > **Audio and Video** in Modern View to create your Audio PIN.

- Your PIN is the last level of protection for prevention of unauthorized access to your personal conferencing account. If a person gains unauthorized access to the host access code for a Personal Conference Meeting (PCN Meeting), the conference can't start without the Audio PIN. Protect your Audio PIN and do not share it.

Exhibit C - Best practices while using Zoom

These ZOOM recommended settings, tips and tricks are basic best practices you should consider in protecting the privacy, safety, and the security of state employees and state digital assets and making your teleconference a success. Note: Some of these options and features may not be available to all, depending on agency implementation.

Video:

- Set both Host Video and Participant Video to OFF by default within your Zoom profile meeting settings.
    - **Note: this doesn't mean participants will not be able to display their camera during the meeting. It simply means they will not have their camera turned on by default when they join the meeting.**
    - More information about Zoom settings and how to change them can be found here
- Test your video before the first meeting:
    - Please visit How Do I Test My Video? for more information.

Audio:

- Set to Both (Telephone and Computer Audio), by default within your Zoom profile meeting settings.
    - More about audio settings can be found here.
- Test your audio before your first meeting:
    - Check out, Testing your computer or device audio from Zoom Support if you'd like more information.

Password:

- Consider using a password to further secure entry into your meeting or webinar.
- More information about passwords and how to set them please take a look at: Meeting and Webinar Passwords

Join Before Host:

- If your meeting does not depend on the attendance of the original, scheduling host, then you should enable join before host.
- This setting allows participants to join the meeting prior to the host, or without a host entirely.
    - More information about this setting can be found here
- If the host does not join the meeting or is not logged in when joining, there are no host controls such as recording, mute/unmute all, lock meeting or remove attendees.
- When Join Before Host is on, the host can join the meeting without being logged in. If you are the host, but do not have host controls such as recording, leave the meeting and login in the Zoom application. Start the meeting again from your Meetings list.

- If one meeting is running and someone tries to start a second meeting with join before host on scheduled by the same host:
    - If started by a Zoom Room, the second meeting will start and close the first meeting without warning.
    - If started by the host, they will have the option to close the first meeting and start the second.
    - If started by a participant, they will receive a message the host has another meeting in progress.
- If Waiting Room is turned on in your meeting settings, Join Before Host will not work for your meetings.
- If you would like the meeting to be recorded without the host attending, you will need to turn on Automatic Cloud recording for the meeting.
- **IMPORTANT:** This is enabled (checked) by default.

Waiting Room:

- A waiting room can be used to control entry to a meeting. Participants can be brought in as desired, either one at a time or all at once.
- If you're using Zoom to lecture online, you may want to enable the waiting room.
- Participants can also ensure they are in the correct room, while they're waiting.
- The waiting room also gives attendees a chance to test their audio configuration.
- Join Before Host will be disabled if the waiting room is enabled.
- **IMPORTANT:** After your meeting starts, it is strongly recommended you disable the waiting room, so you no longer have to manage entry into the meeting. If a participant leaves the meeting and then rejoins, they will need to be allowed back into the meeting.
    - For more information about how to disable the waiting room after the meeting has begun, navigate here.
    - Please visit Zoom Support to learn more about how to customize the waiting room.

Alternative Hosts:

- Alternative Hosts can be listed when scheduling a Zoom meeting.
- Set back up participants as Alternative Hosts just in case the scheduling Host is unable to attend. This allows others to start meetings if necessary, or if the meeting doesn't depend on the original Host.
    - **IMPORTANT:** If the meeting is not dependent on the scheduling Host, it is best practice to designate Alternative Hosts during the scheduling of a meeting or have Join Before Host enabled. Meetings will not begin if the scheduled Host is unable to attend, there are no Alternative Hosts listed, and Join Before Host is disabled.
- In the case of the scheduling Host being absent, the first Alternative Host to join the meeting will assume the role of Host.
- The scheduling Host can reclaim host controls by going to the Participants list and select 'Reclaim Host'. Or, the person with the Host role can assign the Host role back to the intended Host and revert to a participant. In either scenario, the Host can always assign a Co-Host role to any participant.

- In a Webinar, if the Host is reclaimed (or reassigned), the person leaving the Host role will become a Panelist. The new Host can assign any Panelist a Co-Host role to facilitate managing the participants and starting the recording.
- More information about Alternative Hosts can be found here.

Promote Co-hosts to help manage large meeting logistics

- Meetings can have only one Host, but many Co-hosts.
- Co-host is a role the meeting host can assign to any participant during the meeting.
- An attendee can be promoted to a Co-host role after the meeting has started.
    - For more information about how to promote meeting participants to Co-host role please visit Using Co-host in a Meeting from Zoom Support.
- Co-hosts are a good idea for large meetings as they can watch for raised hands, respond to chat messages, and manage breakout rooms.
    - If you're curious how to add Co-hosts to your meeting, please check out Enabling and Adding a Co-host on Zooms support page.
    - For more on the differences between Host and Co-host controls please visit here.

Utilize Breakout rooms for collaboration:

- Breakout rooms are only available in Zoom Meetings.
- Meetings can have up to 50 breakout rooms
- Breakout rooms can have a maximum number of 100 participants per room
    - This number can be increased to 200 if you have one of the large meeting (cap: 500, 1000) add ons.
    - For more information about Zoom add ons please click here.
- Breakout rooms can be randomly selected, or they can be set before the meeting starts.
    - For more information about how to Get Started with Breakout room please visit: Getting Started With Breakout Rooms.
    - For more information about how to manage participants and Breakout rooms in general please visit: Managing Breakout Rooms.
    - If you would like further information about how to participate in Breakout rooms please visit: Participating in Breakout Rooms.

Annotate during your meeting to highlight important information.

- If you're using the Zoom Desktop application or the Zoom mobile application, you can use the annotation tool or whiteboard to help highlight your shared materials.
    - More information about how to annotate during a Zoom meeting please click here.

General Zoom Hosting Tips:

- Speak clearly and do not rush

    - Slowing your delivery will help ensure meeting attendees can comprehend what you're saying. Remember, some attendees may be working with a slower internet speed or lower bandwidth and speaking clearly without rushing can help those with comprehension.
- Animate your delivery
    - Inflection and tone changes can help draw participants into your meeting or lecture.
- Visualize your participants
    - Treat your students or attendees as if they are still right in front of you. Ask attendees questions directly to foster participation and collaboration.
- Look at the whole screen/feature set. Do not focus on just the content area.
    - Make sure either the host or supporting staff (co-host) is set to handle chat, polling or other meeting logistics so attendees can be fully engaged and given the proper amount of attention.
    - More about in-meeting controls can be found here.
- Encourage participants to ask questions and participate.
    - Furthermore: hosts should ask questions and provide opportunities for interaction.
- Use annotation tools to assist in your delivery.
    - More information about how to annotate during a Zoom meeting can be found here.
- During a meeting, the 'Manage participants' control at the bottom of the screen can be used to remove someone from the meeting or lock the meeting to prevent others from joining (even if they have a Meeting ID and password).

More resources including presentation tips, housekeeping slides, etc. can be found at the Zoom website here: https://support.zoom.us/hc/en-us/articles/209743263-Meeting-and-Webinar-Best-Practices-and-Resources