COMMONWEALTH OFFICE OF TECHNOLOGY

AGENCY CONTACT MEMORANDUM #04162020

TO: **Agency IT Leadership, Technical Contacts**

FROM: **Ruth Day, CIO**

DATE: **April 16, 2020**

SUBJECT: **Zoom Teleconferencing**

The Commonwealth Office of Technology, Office of the CISO has continued to monitor the risk factors associated with the Zoom teleconferencing platform and all efforts made by Zoom to mitigate these risks. Over the past week, Zoom has made available patches that address many of the most critical threats with the platform. While some privacy concerns remain, it is the opinion of the Office of the CISO that the risks have been reduced to a level that allows Zoom to be a much-needed tool for use during these challenging times with appropriate due diligence and an understanding of the residual risks.

On April 2, 2020 and April 7, 2020, Zoom issued patches that addressed the primary vulnerability that would allow for credential theft. These patches have been review by the Office of the CISO and have shown to successfully resolve this risk. Other items concerning privacy have also been addressed but questions around protection of the communication from end to end remain. Agencies may now consider Zoom as a viable mechanism for remote meetings and teleconferencing when the content subject matter is not classified as highly sensitive and due diligence and best practices are applied.

The following best practices should apply to all usage of the Zoom platform:

- Agencies must ensure that the most current client is installed and used maintained at the highest patch level. For most client software, users will be prompted that updates are available and must be advised to accept the installation of these patches. Should the install fail, they should seek assistance through their normal IT support channels to resolve the updates prior to use.
- Where possible, the web-based client should be used instead of installing the local client.
- When establishing a meeting room, ensure that it is set with security to require a passcode or password. Meeting organizers may also leverage a lobby where they control the entry in to the meeting. The goal is to ensure that the attendees within the meeting are known and trusted. This may not be practical for public meetings.
- Meetings should be moderated for untrusted activity such as attempts to post links, share files, or off topic subject matter. The meeting moderator should remove these individuals from the meeting immediately. Collaboration features should only be enabled for the meeting when required.
- Alternate mechanisms should be sought for meetings that involve sensitive or proprietary information due to the outstanding privacy questions surrounding the platform.

By applying these best practices, along with the efforts shown by Zoom to address published vulnerabilities, agencies can leverage the platform as appropriate. The Office of the CISO will continue to monitor for changes that may impact this, or any other platform, for changes that may impact the security of the Commonwealth and will provide guidance as quickly as possible.