COMMONWEALTH OFFICE OF TECHNOLOGY

AGENCY CONTACT MEMORANDUM #04012020

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

FROM: **Ruth Day, CIO**

DATE: **April 8, 2020**

SUBJECT: **Zoom Teleconferencing**

The Commonwealth Office of Technology, Office of the CISO has re-evaluated the Zoom video conferencing platform in light of recently disclosed vulnerabilities and concerns over data privacy. Zoom has acknowledged these concerns and has committed to resolve them but at this time there is a high potential for risk.

The published vulnerabilities have the high potential to allow an attacker to target an unsuspecting Commonwealth user with a carefully crafted Zoom message that could allow the user credentials to be compromised or execute malicious code on the victim computer. At a time where large scale use of technologies such as desktop virtualization and virtual private network are in use, compromised credentials can place your agency and the Commonwealth at great risk to threats such as data exposure and ransomware.

It is the ***strong*** recommendation from the Commonwealth Office of Technology, Office of the CISO that agencies refrain from using Zoom until it can be determined that the vulnerabilities have been addressed and all clients have been patched to resolve this concern. The Commonwealth has more secure alternatives such as Microsoft Teams and Amazon Chime that can assist in meeting telecommuting needs of the agencies. For additional information, please reach out to the Commonwealth Service Desk via email at CommonwealthServiceDesk@ky.gov for information concerning these options.

Should agency have a dependence on Zoom for critical meetings, the following steps can be taken to help reduce risk but should not be considered as an elimination of risk:

- When establishing a meeting room, ensure that it is set with security to require a passcode or password.
- Alternatively, use a lobby for the room that requires that a meeting moderator allow entry in to the room to validate attendees.
- Advise all participants in meeting to not provide, or click, on any links within the meeting.

While these steps will help manage some levels of risk, they do not completely mitigate it. Agencies are strongly encouraged to leverage alternative methods where possible.