CAROLYN B. MALONEY
CHAIRWOMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225-5051
MINORITY (202) 225-5074
http://oversight.house.gov

April 10, 2020

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
2157 Rayburn House Office Building
Washington D.C. 20515

Dear Chairwoman Maloney:

As you know, Zoom is a user-friendly video teleconferencing system that allows businesses to continue to work and connect employees during this time of social distancing and increased teleworking. Zoom is also being used by teachers to keep in touch with students and conduct online classes.[1] While used by a number of groups for virtual work conferencing prior to the pandemic, Zoom has become a household name during the COVID-19 pandemic as users are hosting everything from workouts to virtual happy hours on its platform.

Unfortunately, such ubiquity has also exposed concerns with Zoom's cybersecurity protocols. There have been many reports of "Zoom-bombing" that include video conferences being interrupted by hate speech and pornographic images.[2] Zoom is also being used to distribute malware.[3] These reports prompted the Federal Bureau of Investigation (FBI) to issue a security warning to people using Zoom's platform urging users to take specific precautions to secure their computers and networks.[4] This week, the Senate Sergeant at Arms wrote that Zoom poses the

[1] Melanie Burney, *How teachers are using technology to keep in touch with students during coronavirus school closures*, PHILADELPHIA INQUIRER (Mar. 24, 2020), https://www.inquirer.com/health/coronavirus/coronavirus-nj-education-schools-technology-coping-teachers-outreach-cherry-hill-20200324.html.
[2] Press Release, Federal Bureau of Investigation, FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic (Mar. 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.
[3] Maggie Miller, *Researchers see spike in suspicious Zoom domains during coronavirus pandemic*, THE HILL (Mar. 30, 2020), https://thehill.com/policy/cybersecurity/490220-researchers-see-spike-in-suspicious-zoom-domains-during-coronavirus.
[4] Press Release, Federal Bureau of Investigation Boston Office, FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic (Mar. 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

threat of "potential compromise of systems and loss of data, interruptions during a conference, and lack of privacy."[5]

In addition to reports of hacking and malware, a large portion of Zoom's research and development work is done by employees in China. In Zoom's S-1 filing for their initial public offering (IPO), Zoom stated "we have a high concentration of research and development personnel in China, which could expose us to market scrutiny regarding the integrity of our solution or data security features."[6] As of January 31, 2019, Zoom reported employing over 500 people in China, operations that Zoom expected to expand post-IPO.[7] Zoom has made a business decision to concentrate these operations in China because of cheaper labor costs compared to the United States. Zoom stated "[i]f we had to relocate our product development team from China to another jurisdiction, we could experience, among other things, higher operating expenses, which would adversely impact our operating margins and harm our business."[8]

Despite these issues and the FBI warning, on Friday, March 27, 2020, you noticed an official Committee meeting for Members using the Zoom teleconference system with the Department of Health and Human Services (HHS) and the Federal Emergency Management Agency (FEMA).[9] At the time, HHS and FEMA raised concerns about Zoom's security and objected to hosting any Member meeting on the Zoom platform. This Member briefing was eventually changed to a moderated conference call using HHS conferencing system.[10]

Then, in spite of the warnings by the FBI and media outlets,[11] on April 3, 2020, you held a Zoom-hosted Member briefing on women's rights in Afghanistan with the Special Inspector General for Afghanistan Reconstruction (SIGAR).[12] During this important briefing, the session was "Zoom-bombed" at least three times. The impact of hacking and malware on Member and staff devices is still being determined.

The lack of cybersecurity controls at Zoom has led the Senate Sergeant at Arms to not use Zoom or any other video conferencing technology outside Senate-supported technologies.

---

[5] Cristiano Lima, Internal Senate memo warns Zoom poses 'high risk' to privacy, security, Politico (Apr. 9, 2020), https://www.politico.com/news/2020/04/09/internal-senate-memo-warns-zoom-poses-high-risk-to-privacy-security-177347.

[6] Zoom Video Communications, Inc., Registration Statement (Form S-1) 21 (Mar. 22, 2019), https://www.sec.gov/Archives/edgar/data/1585521/000119312519083351/d642624ds1.htm.

[7] *Id*, 23..

[8] *Id*, 25..

[9] Full Committee Member Notice: Full Committee Member Briefing with FEMA and HHS re: Coronavirus Crisis (Mar. 27, 2020) (on file with the Committee).

[10] *See*, Revised Full Committee Member Notice: CHANGE FROM ZOOM TO CONFERENCE CALL MODERATED BY HHS (Mar. 29, 2020) (on file with the Committee).

[11] See, Maggie Miller, *Zoom vulnerabilities draw new scrutiny amid coronavirus fallout*, THE HILL (Apr. 2, 2020), https://thehill.com/policy/cybersecurity/490685-zoom-vulnerabilities-exposed-as-meetings-move-online. Also see, Zak Doffman, *New Zoom Security Warning: Your Video Calls At Risk From Hackers—Here's What You Do*, FORBES (Jan. 28, 2020), https://www.forbes.com/sites/zakdoffman/2020/01/28/new-zoom-roulette-security-warning-your-video-calls-at-risk-from-hackers-heres-what-you-do/#3d42cfbf7343.

[12] Full Committee Member Notice: Zoom Briefing with SIGAR John F. Sopko on Women's Rights in Afghanistan (Apr. 1, 2020) (on file with the Committee).

While Zoom may have a product suitable for government use, the Senate Sergeant at Arms noted no Zoom product was vetted or cleared for use by Senate offices.[13]

Given the concerns surrounding Zoom's security, it is clear Zoom is not an appropriate platform for Committee business, which may be particularly sensitive during the COVID-19 pandemic. Please immediately suspend any current or future use of Zoom systems for official committee activities and take immediate steps to evaluate the Committee's internal cybersecurity preparedness to prevent hackers from accessing sensitive committee information through the Zoom platform.

Sincerely,

Jim Jordan
Ranking Member
House Committee on Oversight and Reform

[13] *Supra*, note 5.