90-Day Security Plan: Key Updates as of July 1, 2020

On April 1, 2020, we **pledged** to make a number of enhancements to address security and privacy. The 90-day program we announced on that day refocused our company on 7 commitments that embedded security and privacy permanently in Zoom's DNA. Here is a status update on each of those commitments:

#1: Enact a feature freeze, effective April 1, and shift all our engineering resources to focus on our biggest trust, safety, and privacy issues.

Status: We enacted a 90-day feature freeze on all features not related to privacy, safety, or security. We released **Zoom 5.0**, featuring AES 256 GCM encryption, the Security icon and the "Report a User" feature, changed default settings for meetings (turning on passwords and waiting rooms by default), tighter Zoom Chat controls, and more. We also **acquired Keybase**, started building our end-to-end encryption offering for all users (free and paid), and began offering **customized data routing** by geography.

#2: Conduct a comprehensive review with third-party experts and representative users to understand and ensure the security and privacy of all of our new use cases.

Status: We have worked with a group of third-party experts to review and make enhancements to our products, practices, and policies, including our CISO advisory council, Lea Kissner, Alex Stamos, Luta Security, Bishop Fox, Trail of Bits, NCC Group, Praetorian, Crowdstrike, Center for Democracy and Technology, and other organizations in the privacy, safety, and inclusion spaces.

#3: Prepare a transparency report that details information related to requests for data, records, or content.

Status: We have made significant progress defining the framework and approach for a transparency report that details information related to requests Zoom receives for data, records, or content. We look forward to providing the fiscal Q2 data in our first report later this year. In the meantime, we have recently released a **Government Requests Guide** and we also updated our privacy policies, mostly to make them easier to understand. These documents can be found on **zoom.com/privacy-and-legal**.

#4: Enhance our current bug bounty program.

Status: We have developed a Central Bug Repository and related workflow processes. This repository takes vulnerability reports from HackerOne, Bugcrowd, and **security@zoom.us** (the latter of which does not require an NDA) triaged through Praetorian. We established an ongoing review process with daily meetings, and improved our coordination with security researchers and third-party assessors. We also hired a Head of Vulnerability and

Bug Bounty, several additional appsec engineers, and are in the process of hiring more security engineers, all dedicated to addressing vulnerabilities.

#5: Launch a CISO council in partnership with leading CISOs from across the industry to facilitate an ongoing dialogue regarding security and privacy best practices.

Status: We launched our CISO council, led by our Global Deputy CIO Gary Sorrentino and composed of 36 CISOs from a variety of industries, including SentinelOne, Arizona State University, HSBC, and Sanofi. This council has met four times over the past three months and advised on important matters such as regional data center selection, encryption, meeting authentication, and key security features.

#6: Engage a series of simultaneous white box penetration tests to further identify and address issues.

Status: Zoom engaged multiple firms - Trail of Bits, NCC Group, and Bishop Fox - to review our entire platform. Their scope of work covered Zoom's production environment, core web application and corporate network, and the public API for common clients.

#7: Host a weekly webinar on Wednesdays to provide privacy and security updates to our community.

Status: We have hosted a total of 13 webinars, every Wednesday since April 1st, featuring a number of our executives and consultants who took live questions from the attendees.

Other key updates:

- We made several key leadership additions or changes since April 1, including:
  - **Velchamy Sankarlingam**, President of Product and Engineering
  - **Jason Lee**, Chief Information Security Officer
  - **Damien Hooper-Campbell**, Chief Diversity Officer
  - **H.R. McMaster** added to the Zoom Board of Directors
  - **Josh Kallmer**, Global Head of Public Policy and Government Relations
  - Head of Vulnerability and Bug Bounty, starts 7/13
  - Andy Grant, Head of Offensive Security, starts 7/13
- **Zoom Phone added to Zoom for Government**, which is already authorized under the U.S. Federal Risk and Authorization Management Program (FedRAMP)
- We remain committed to significantly growing our US-based engineering team to support increased usage with **new offices** based in Phoenix, Arizona and Pittsburgh, Pennsylvania