Key Zoom Features for Secure Meetings

Zoom is committed to providing a safe and secure communications platform that allows users and administrators to customize their security and experience via easy-to-use settings. We have engaged some of the industry's top security professionals and our clients to advise us as we continue to develop our products and services given that we are now supporting so many different use cases. Some of our most notable security features include:

- **Encryption** of data in transit and at rest is currently AES 256 ECB migrating to AES 256 GCM on May 30
- **Controlled data routing** that allows paying customers to opt-in or opt-out of any of our data centres (excluding their home region) and, for enterprise clients, the ability to customize and manage geographic regions for specific meetings
- **Transparency on data routing** via the account administration dashboard
- Safeguards and controls to **prohibit unauthorized participants** such as:
  - Eleven (11) digit unique meeting IDs
  - Complex passwords
  - Waiting Room with the ability to automatically admit participants from your domain
  - Meeting lock feature that can prevent anyone from joining the meeting, and ability to remove participants
  - Authentication profiles that only allow entry to registered users, or restrict to specific email domains
- **Meeting host controls** can enable/disable participants to:
  - Content share
  - Chat
  - Rename themselves
- **Security controls** at the fingertips of the host/co-host with a dedicated Security icon on the main interface
- All cloud **recordings are encrypted** with complex passwords on by default
- Prevent robocalling with **rate limiting and reCAPTCHA** (requires human intervention) enabled across all platforms
- Audio recordings with a user's electronic fingerprint embedded into the audio as an **inaudible watermark** so if the recording is shared without permission, we can help identify the source
- **Content watermarking** superimposes the image of a meeting participant's email address onto shared content they screenshot

April 23, 2020