I, Josh Parecki, do hereby declare as follows pursuant to 28 U.S.C. § 1786:

I am employed by Zoom Video Communications, Inc. ("Zoom"), in the position of Chief Compliance Officer, Head of Trust and Safety. I am a United States citizen, and I am over 18 years of age. In March 2024, representatives from Zoom for Government, including myself, began working with representatives from United States Attorney's Office for the District of Columbia to develop a set of proposals to afford secure, remote access to verified victims in the case of *United States v. Abu Agila Mohammad Mas'ud Kheir Al-Marimi*. The Zoom for Government team working on this proposal includes representatives holding the titles of Government Solutions Engineer; Head of Public Sector; and Account Executive, Enterprise Federal. A copy of the proposals we have developed is attached to this declaration as Attachment A, and I adopt those proposals as part of this declaration.

The Zoom for Government team is responsible for implementing the Zoom for Government platform, which is specifically designed to be used for United States Government work. The Zoom for Government platform is U.S.-based, managed by U.S. Persons only, and utilizes U.S.-based GovCloud infrastructure and U.S.-based data centers. As such, Zoom for Government is considered a Government Community Cloud (GCC), which is defined by the National Institute of Standards and Technology as a "cloud infrastructure . . . provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations)." In addition, Zoom for Government is authorized The Federal Risk and Authorization Management Program (FedRAMP), which is responsible for providing a standardized approach to security authorizations for Cloud Service Offerings, as a "Moderate Impact" system. "Moderate Impact" systems are appropriate for use where "the loss of confidentiality, integrity, and availability would result in

serious adverse effects on an agency's operations, assets, or individuals. Serious adverse effects could include significant operational damage to agency assets, financial loss, or individual harm that is not loss of life or physical." *See* https://www.fedramp.gov/understanding-baselines-and-impact-levels/.

In the course of preparing these proposals, the Zoom for Government team has consulted with representatives of the Department of Justice involved in the prosecution of this case and has reviewed a copy of this Court's Minute Order dated March 13, 2024. During these meetings, the Zoom for Government team identified the following security requirements for these proposals:

1. Authorized remote observers ("remote observers") must be able to receive video, audio and content feeds from Court proceedings at any location deemed appropriate in real time.

2. The feeds must be one-way, meaning that remote observers cannot communicate during Court proceedings unless explicitly permitted by the Court.

3. Remote observers must not be able to interact with each other during proceedings unless explicitly authorized by the Court

4. Remote observers must be both electronically and visually authenticated prior to being allowed to view court proceedings.

5. A team of government personnel ("monitors") must be able to visually monitor all remote observers throughout Court proceedings.

6. Monitors shall have the ability to pull and subsequently return any remote observer out of the courtroom proceedings into a breakout room to directly and privately communicate.

7. All content, video or audio received by remote observers shall be watermarked with their authenticated username. Any capture of received content will have been identifiable by this watermark.

Attachment A contains three separate proposals that the Zoom Team believes will satisfy the issues that the Court ordered addressed in its March 13 Minute Order. Those proposals contain common authentication and security features, as well as features designed to mitigate the risk of rebroadcasting of the proceedings, as outlined in Attachment A. Security features include the use of U.S.-based infrastructure that is managed by U.S. persons on the Zoom for Government platform; authentication of user identity includes the use of two-factor authentication and the pre-registration of accounts; and features designed to defeat rebroadcasting include the use of audio and video watermarks, unique to each user, which would allow Zoom to assist in identifying the source of any audio and video that may be rebroadcast or distributed without authorization.

The three proposals are intended to provide the Court with a high-level view of what the Zoom for Government platform is capable of, as well as what administrators, moderators, and the remote users would expect in each scenario. Zoom's existing infrastructure can accommodate all three proposals. If the Court chooses to proceed with the Zoom for Government platform to afford remote access for victims in this case, the Zoom for Government team is ready to test, fine-tune, and validate the option it chooses with court and/or government personnel, followed by additional tailored recommendations if necessary. The Zoom for Government team plans to remain available to the government and the Court if there are any questions about the proposals in Attachment A and to assist, to the extent feasible, in implementing any such proposal the Court may adopt.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on May 31, 2024.

DocuSigned by:
Tosa Parecki
B36F529A0DE8454...

ATTACHMENT A

Zoom's Proposals to Securely Provide Remote Observer Access to Court Proceedings

Overview

The purpose of this document is to outline Zoom's comprehensive proposal to permit victims remote access to pretrial proceedings and trials in a secure manner that will not jeopardize the safety or the integrity of such proceedings.

Here we explain in detail Zoom features the Court and the United States can use to: (1) minimize the risk of unauthorized persons from gaining access to the Court's proceedings; and (2) prevent recording, (re)distribution, or broadcasting of the Court's proceedings. We will also provide an understanding of the resources, including personnel and facilities, the Court and the United States may dedicate to achieve these ends.

Requirements

The following security requirements were shared with Zoom by the United States:

1. Authorized remote observers ("remote observers") must be able to receive video, audio and content feeds from Court proceedings at any location deemed appropriate in real time.
2. The feeds are one-way, meaning that remote observers cannot communicate during Court proceedings unless explicitly permitted by the Court.
3. Remote observers must not be able to interact with each other during proceedings unless explicitly authorized by the Court
4. Remote observers must be both electronically and visually authenticated prior to being allowed to view court proceedings.
5. A team of government personnel ("monitors") must be able to visually monitor all remote observers throughout Court proceedings.
6. Monitors shall have the ability to pull and subsequently return any remote observer out of the courtroom proceedings into a breakout room to directly and privately communicate. Some examples of reasons a monitor may need to communicate directly with remote observers include to:
    a. address a possible violation of room security guidelines;
    b. request grief counseling or some other type of support; or
    c. any other reason a Monitor may determine.
7. All content, video or audio received by remote observers shall be watermarked with their authenticated username. Any capture of received content will have been identifiable by this watermark.

Proposed Solutions

In this section, Zoom will present and describe several possible solutions to address all or most of the requirements outlined in the previous section. Please note, there is no way for Zoom technology to physically secure the remote environments from which remote observers join. To help minimize this risk, we suggest monitors visually inspect the remote observers' physical environment via the remote observers' camera's field of view.

Certifications

All proposed solutions below are based on the existing capabilities of the Zoom for Government ("ZfG") platform. ZfG is intended to be used by and for US Government activities. As such ZfG is considered a Government Community Cloud (GCC) by NIST definitions (see https://csrc.nist.gov/glossary/term/community_cloud). Moreover, ZfG is FedRAMP Moderate authorized, and ZfG is U.S.-based, managed by U.S. Persons only, and utilizes U.S.-based GovCloud infrastructure and U.S.-based data centers.

Authentication

For each of the below proposed solutions, Zoom recommends the Court require authenticated entry only. By leveraging authentication upon entry and restricting guests or unauthenticated user accounts from joining Court proceedings, this would mitigate risk of unauthorized attendees. It requires each remote observer to register with the account owner / admin prior to Court dates so that a specific user account can be created for each registered remote observer. Please note, this feature is available at no additional licensing cost, but there may be additional administrative burden in assigning licenses to remote observers. There are differing levels of authentication and multiple available authentication platforms (i.e. Zoom of other 3rd party integrations). At minimum, however, Zoom recommends that some form of Two-Factor Authentication ("2FA") be leveraged with whatever authentication platform is selected.

Other Security Measures

For each of the proposed solutions outlined below, Zoom recommends the Court enable watermarking for all video, content and audio. The video watermark feature superimposes an image, consisting of a meeting participant's email address, onto the shared content they are viewing and over their video. The audio watermark, or audio signature, is an inaudible watermark of a user's personal information embedded in the audio that is played through the receiving user's speakers by the client receiving audio from Zoom meeting servers. This means that if someone records the meeting, with either a separate microphone or 3rd-party, and shares the audio file without permission, Zoom can assist with determining which participant was responsible.

Phone (PSTN) dial-in can be provided for remote observers that are not able to utilize the Zoom Desktop application or who do not have PC audio capabilities. The monitor will see a remote

number identified for that call-in the observer, as long as the phone carrier provides the calling number as part of their service. The accuracy of that number will also be dependent on the phone carrier being used. Zoom can only display the number that is delivered in the call setup. We can not validate the number. Audio Watermarking would not be available for Phone (PSTN) call-in observers.

Proposed Solution One: Webinar with breakout rooms proposal

Solution one leverages Zoom's Webinar product. From an administrative perspective, this Solution is the easiest to set up and manage. By default, a Webinar is designed to accommodate a one-to-many or auditorium-style meeting, and it allows a maximum of 50,000 participants. Webinar also provides for three types of participants, all of which can be pre-assigned prior to the court session. They are:

- **Hosts/Co-Host**s: hosts/co-hosts have administrative rights over the meeting and can act as meeting monitors in this Solution;
- **Panelists**: panelists are participants that have the ability to transmit video, audio and content into the meeting and is way the Court would join the meeting in this Solution;
- **Attendee**: attendees are participants that join the meeting as receive-only participants (e.g., no video, audio or content) and would be the remote observers in this Solution.

As noted, remote observers would be in the attendee role in this Solution. Monitors will be in the host / co-host role. Monitors can enable two-way chat communication with remote observers to address a circumstance where a remote observer may need assistance. Remote observers, however, will not have the ability to chat or communicate in any way with any other participant.

Monitors have the ability to set up a number of breakout rooms to accommodate the circumstance where a remote observer is in need of assistance in a manner exceeding the limitations of the chat feature. Monitors can invite a remote observer into a private session in a breakout room without disturbing ongoing Court proceedings using this feature. After the monitor and remote observer have completed their private session the monitor can move the remote observer back into the Court proceedings where they would be reverted to receive-only mode. Separately, Webinars support a "backstage" function that would allow the monitors to communicate on a separate channel outside of the court proceedings.

Reauthentication at the beginning of each trial day or for any reason would be the same process as described when initially joining the session. Zoom could only validate they are logged in and authenticated via two-factor authentication and there would be no visual authentication.

Summary: This Solution would be easiest to set up and manage, however, it does not meet all of the requirements outlined above. Specifically, it does not provide an easy mechanism for visual authentication or visual monitoring of remote observers' remote physical locations.

Proposed Solution Two: Controlled Meeting with breakout rooms

Solution two leverages Zoom's Meeting product. In Meetings, participants have the ability to transmit as well as receive video and audio regardless of role, and there is a maximum of 1000 participants.

Meetings provide three mechanisms for authentication of the remote observers. First, Meeting settings allow monitors to require specific user credentials to login to the Zoom app and join the Court proceedings. Second, monitors may require a waiting room during Court proceedings. This feature will cause remote observers to congregate in a virtual waiting room prior to being allowed into the proceedings in a waiting room. Monitors can visually authenticate remote observers while they are in the waiting room and can visually confirm whether there are any uninvited participants in the remote space before letting a remote observer into the proceedings. Third, monitors can move remote observers into waiting rooms to facilitate the same visual authentication processes available within a waiting room at any time during the proceedings.

By default, the meeting product is designed for free-flowing back-and-forth communication among participants. Meetings can, however, be pre-configured into "Focus" mode limiting remote observers to see monitors but not each other. Monitors can also mute remote observers' microphones and control the ability of remote observers to unmute themselves. In effect, these settings create a Webinar-like one-to-many experience, and like the Webinar solution, remote observers can chat to a monitor if they need assistance. Monitors can then pull a remote observer into a Breakout room to communicate and then move them back to the court session when appropriate. Of note, monitors can only see up to 25 video feeds on the screen at any time. If there are more than 25 remote observers, a new page view is created and the monitor will need to page over to monitor the additional remote observers. For example if there are 200 remote observers, the monitor would have eight pages of video feeds to navigate.

Reauthentication at the beginning of each trial day would be the same process as described when initially joining the session on Day 1 of the Court proceedings. If the Court wanted to reauthenticate remove observers after breaks the monitor could move each observer to a pre-designated breakout room when the Court proceedings break. Monitors would then communicate with the remote observers in the breakout room and repeat the visual authentication process described above shortly before Court proceedings begin again. Once completed, they could be moved from their breakout to the courtroom session.

Summary: While this Solution potentially meets all the requirements outlined in the previous section, it also has the most administrative overhead. This Solution would require additional monitor training to keep the logistics smooth and depending on the number of observers, the Court may require multiple monitors. Also, in this solution, all remote observers would need to be authenticated and settled in their virtual space before the Court proceedings begin. And, unfortunately, there isn't a good solution for observers joining after the session begins. This lack of solution is particularly true should the Court take our recommendation to lock the meeting once the proceedings begin to further minimize the risk of disruption. In effect, locking the meeting is comparable to locking the doors to the courtroom and barring any late attendees.

Proposed Solution Three: Multiple Meeting proposal

Solution three also leverages the Meetings product but unlike Solution two, we propose two separate meetings. A meeting for the visual authentication process and a meeting for Court proceedings. In this proposal, remote observers would be invited to a meeting where monitors would perform a visual authentication process, just as in Solution two. Remote observers would only see the monitors but not each other. Once authenticated, they would be dropped from the authentication meeting and be manually connected into the Court proceeding. As an additional security precaution, this Solution hides the Court proceeding meeting link from the remote observers or anyone in the public. Remote observers will join the Court proceedings when they receive an incoming call. Thereafter, the experience and feature recommendations are identical to Solution two.

Reauthentication at the beginning of each trial day would be the same process as described when initially joining the session on Day 1 of the trial. If the Court wanted to reauthenticate remove observers after breaks the monitor could move each observer to a pre-designated breakout room when the Court proceedings break. Monitors would then communicate with the remote observers in the breakout room and repeat the visual authentication process described above shortly before Court proceedings begin again. Once completed, they could be moved from their breakout to the courtroom session.

Summary: Solution three potentially meets all the requirements outlined, eliminates some of the complexity and risk of using a single session to accomplish the authentication process and allows a path for people joining after the Court proceedings have begun.

User Experience for each proposed solution

Proposed Solution One: Remote Observer Experience

Weeks before the trial: Remote observer registers with USDOJ and a user account (with authentication) is created for that observer. The Court or the Government can potentially create a webinar to provide pre-trial training.

Days before the trial: Remote observer receives an invite via email with a unique link to join the webinar.

Day of trial: Remote observer joins the webinar and is placed in the waiting room until court proceedings begin. They will be able to watch the courtroom feeds (video, audio, content). They will have the ability to chat with monitors or raise their hand if they need assistance. They will be dropped when court proceedings end.

Reauthentication process: It may be necessary to re-authenticate remote observers at the beginning of each day or after breaks. In solution one, the only authentication available is via two-factor authentication. Therefore, to reauthenticate, the Monitors should drop the remote observers from the webinar and ask them to rejoin. This process would validate their login authentication.

Proposed Solution Two: Remote Observer Experience

Weeks before the trial: Remote observer registers with USDOJ and a user account (with authentication) is created for that victim/individual. The Court or the Government can potentially create a webinar to provide pre-trial training.

Days before the trial: Remote observer receives an invite via email with a unique link to join the meeting.

Day of trial: Remote observers use the provided link to join the meeting and are placed in a waiting room until a Monitor allows them in and moves them to a breakout room for visual authentication and room inspection. Once authenticated, they will be virtually seated in the courtroom and wait for proceedings to begin. Remote observers will be able to watch the courtroom feeds (video, audio, content). They will have the ability to chat with Monitors or raise their hand if they need assistance. They will need to keep their camera on as they will be monitored.

Reauthentication process: It may be necessary to re-authenticate remote observers at the beginning of each day or after breaks. At the beginning of the day, remote observers will follow the same process described in the "Day of Trial" but during the day, remote observers may be given the option to disconnect from the session should there be a break. Remote observers would then need to join and re-authenticate again as they did at the beginning of the day. They may also be given the option to stay connected to the session. If they chose to stay connected, the monitors would need to move the remote observers into a breakout room during the break. And, if re-authentication is required, monitors could do so in the breakout rooms prior to their re-entry into the Court proceedings.

Proposed Solution Three: Remote Observer Experience

Weeks before the trial: Remote observer registers with USDOJ and a user account (with authentication) is created for that observer. The Court or the Government can potentially create a webinar to provide pre-trial training.

Days before the trial: Remote observer receives an invite via email with a unique link to join the pre-authentication meeting.

Day of trial: Remote observer uses the provided link to join the authentication meeting and are placed in a waiting room until a monitor allows them in and moves them to a breakout room for visual authentication and room inspection. Once authenticated, they will be disconnected from the call and will wait for an incoming call on the Zoom application. When the remote observer

receives the incoming call, they will hit the answer button and will be virtually seated in the courtroom and wait for proceedings to begin. They will be able to watch the courtroom feeds (video, audio, content). They will have the ability to chat with Monitors or raise their hand if they need assistance. They will need to keep their camera on as they will be monitored.

Reauthentication process: It may be necessary to re-authenticate remote observers at the beginning of each day or after breaks. At the beginning of the day, remote observers will follow the same process described in the "Day of Trial" but during the day, remote observers may be given the option to disconnect from the session should there be a break. Remote observers would then need to join and re-authenticate again as they did at the beginning of the day. They may also be given the option to stay connected to the session. If they chose to stay connected, the monitors would need to move the remote observers into a breakout room during the break. And, if re-authentication is required, monitors could do so in the breakout rooms prior to their re-entry into the Court proceedings.

Overall Summary

This document was intended to provide some possible solutions to the request that Lockerbie victims be able remotely watch the pretrial proceedings and trial, without jeopardizing the safety or the integrity of such proceedings. While there is no way the proposed solutions can provide 100% certainty that the remote locations are secure, we have presented a few solutions that could leverage two way video communication to provide some level of assurance.

The outlined proposed solutions are fairly high level proposals that, should there be interest in proceeding, would need to be tested and validated with Court or Government personnel. We expect a level of fine tuning and testing of proposed solutions would be necessary and we could make additional recommendations based on this testing.