GOVERNMENT, SECURITY & PRIVACY

Securing the Zoom for Government Platform

Matt Mandrgoc
August 2, 2022 · 5 min read

Security needs to be present at the start of any program, process, and product. This goes for any organization across every industry, but nowhere is it more vital to our national well-being than the public sector.

Today's government agencies need solutions that help protect the exchange of important and sensitive information, all with the right controls in place for compliance. That's where Zoom for Government comes into play.

Specifically designed with federal security requirements in mind, our Zoom for Government platform comes with key security features and helps support relevant compliance requirements to facilitate safe and secure government operations.

Here's a look at six key ways Zoom for Government works to protect your information.

1. End-to-end encryption (E2EE)

Zoom Meetings

When enabled, this feature uses Zoom's standard 256-bit AES-GCM encryption to help encrypt communication between all authenticated meeting participants using the Zoom for Government client. The difference is that the cryptographic keys are known only to the devices of the meeting participants. This means that third parties — including Zoom — do not have access to the meeting's private keys.

Zoom Phone

Zoom for Government users also have the option to upgrade to E2EE during one-on-one Zoom Phone calls between users on the same Zoom for Government account that occur via the Zoom client. During a call, you can select "More" and see an option to elevate the session to an end-to-end encrypted phone call. When enabled, E2EE establishes that the call is encrypted using cryptographic keys known only to the devices of the caller and receiver. Additionally, users will have the option to verify E2EE status by providing a unique security code to one another.

2. A growing list of certifications

Zoom for Government has been authorized at the FedRAMP Moderate Level and achieved a Provisional Authorization (PA) from Defense Information Systems Agency (DISA) for the Department of Defense (DoD) at Impact Level 4 (IL4) and an Authorization to Operate (ATO) for DoD IL4 for Zoom Meetings with the Department of the Air Force. Zoom for Government also helps to support HIPAA and CJIS compliance.

While these authorizations are specific to Zoom for Government, commercial Zoom has also attained other relevant attestations, all of which you can learn about on our Trust Center.

3. Nomadic E911

Zoom Phone for Government offers an enhanced 911 (E911) feature that can be used to direct emergency services to an exact location when a 911 call is placed. With Zoom's Nomadic E911, Zoom Phone soft and hard phones can help dynamically track the location of users as they move around a facility, keeping their location up to date in the event of an emergency.

Nomadic E911 — which comes included in Zoom Phone — helps today's government agencies comply with RAY BAUM's Act, which tasks today's organizations with automatically reporting a dispatchable location for personnel safety. This feature is especially important as agencies embrace flexible work, helping keep employees safe no matter where they are.

For details on how to configure Nomadic E911 on Zoom Phone, check out this guide.

4. U.S.-based staff and data centers

Zoom for Government leverages the U.S.-based AWS GovCloud infrastructure and U.S.-based co-located data centers. It is deployed and managed by U.S. persons only. This feature is exclusive to Zoom for Government and not available for commercial Zoom.

5. Watermarking

To help protect the privacy of confidential information shared during a meeting and prevent leaks, meeting hosts can enable two types of Zoom watermarks:

- Image watermarks superimpose an image on a shared screen, which consists of a portion of a meeting participant's own email address. This image is splashed across the content a person is presenting, as well as their video.
- Audio watermarks embed a user's info as an inaudible mark in any offline recording of a meeting. If the audio file is shared without permission, Zoom can help identify which participant recorded the meeting.

6. Authenticated login

To help authenticate Zoom for Government users as they log into the client, we offer a single sign-on (SSO) feature that creates a safe and quick login process. If you can not use single sign-on, we recommend using two-factor authentication (2FA) to still add an extra layer of security to the process. SSO and 2FA are fundamental for enabling a zero-trust architecture, which has been identified as key for strengthening agencies' security posture.

Supporting the public sector's security posture

These are just a handful of security features and authorizations that come with Zoom for Government, and most are available on commercial Zoom, too. From existing in-meeting security controls to privacy notifications, both Zoom for Government and commercial Zoom come with countless features designed to make security a seamless part of government communications.

Government work relies on effective and secure communication. Whether you're conveying important policy changes or collaborating with personnel on an upcoming mission, government workers can rely on Zoom for Government to help facilitate the safe exchange of important information without having to sacrifice speed, flexibility, and experience. Agencies can operationalize flexible work while simultaneously strengthening the security posture of the public sector.

Learn more about Zoom for Government by visiting our webpage or find us on the FedRAMP Marketplace.

Editor's note: This post was updated on 8/2/22 to reflect the latest security information for Zoom for Government.