

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:

COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE •
JOINT COMMITTEE ON TAXATION

May 12, 2021

Katy Kale
Acting Administrator
General Services Administration
1800 F St., NW
Washington, DC 20405

Dear Acting Administrator Kale:

To learn more about the effectiveness of security audits for software approved for government use, I write to request a copy of the “security package” for Zoom, detailing the security assessment of this popular video conferencing service. It is extremely concerning that after Zoom was cleared for government use by the General Services Administration (GSA) in April 2019, security researchers discovered multiple serious vulnerabilities in the year that followed.

GSA operates the Federal Risk and Authorization Management (FedRAMP) program, which seeks to reduce unnecessary red tape for federal agencies using commercial cloud technologies. In particular, FedRAMP enables federal agencies to use commercial cloud services that have already been evaluated by other government agencies without having to re-evaluate the security of those services.

According to information provided to my office by GSA, U.S. Customs and Border Protection (CBP) was the first agency to issue an Authorization to Operate for Zoom for Government in February 2019. As part of this process, a third-party auditor was hired to conduct an assessment of Zoom’s service for government agencies, which included Zoom’s desktop and mobile software. These are the same for government users and consumers. After receiving the results of this security audit, CBP gave Zoom’s software the green light. Two months later, GSA granted Zoom for Government approval in the FedRAMP program, enabling other government agencies to use the company’s product without conducting their own security assessment.

In July 2019, a security researcher revealed a major flaw in Zoom’s software for Mac computers, which malicious websites could exploit to forcibly join a victim to a Zoom call, with their video camera activated, without their permission. The vulnerability revealed by the researcher was so bad that Apple pushed out its own emergency update to all users, removing the vulnerable Zoom software, rather than waiting for Zoom to do so. This was not the only vulnerability discovered in Zoom’s software after GSA approved Zoom for federal use. In the spring of 2020, as the impact of the COVID-19 pandemic forced a rapid migration to work-from-home and tens of

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

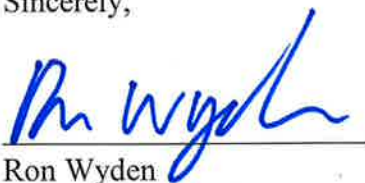
PRINTED ON RECYCLED PAPER

millions of people began regularly using Zoom, researchers discovered and disclosed several other serious vulnerabilities in Zoom's desktop and mobile software.

That researchers were able to discover so many serious security flaws in Zoom's software after that software had been audited as part of the certification process for government use raised serious questions about the quality of FedRAMP's audits. That is why in June 2020, I requested a copy of the security package provided by GSA to government agencies documenting the results of the audit and other relevant information regarding the steps taken to evaluate Zoom's software. GSA refused my request. As there is now a new administration, and I now serve as Chairman of the Senate Committee on Finance, I am renewing the request.

If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator



Ms. Gianelle E. Rivera
Associate Administrator
U.S. General Services Administration
1800 F Street NW
Washington, D.C. 20405

June 11, 2021

Dear Ms. Rivera:

Thank you for your June 2, 2021 letter, and for the opportunity to provide you with Zoom's views regarding the possible disclosure of Zoom's FedRAMP security package (the Security Package) to Senator Wyden's office outside of the standard disclosure procedure for such security packages.

As Senator Wyden mentions in his recent letter to the General Services Administration (GSA), when he previously requested disclosure of Zoom's security package in July 2020, GSA refused this request. In the current instance, Zoom sees no new facts or circumstances that would warrant GSA changing its previous decision not to disclose Zoom's Security Package. Disclosing Zoom's Security Package outside of the standard process would set a dangerous precedent that would undermine the special trust and confidence that all Cloud Service Providers place in the FedRAMP process when they submit proprietary and confidential information in support of FedRAMP certification.

Zoom's Security Package and related documents provide specifics regarding the security associated with the Zoom for Government product that is exclusively available to federal, state, and local government entities and approved federal contractors. Access is restricted to the Security Package and related documents that are housed in the max.gov repository, and Zoom submitted those materials with the understanding that this repository's access is restricted to government agencies or related entities only for their use in making authorization decisions for use of the Zoom for Government product. Any disclosure outside of these narrow purposes puts at grave risk the very foundation of trust between the Cloud Service Providers and the FedRAMP office.

Zoom takes the security of its products and transparency with customers very seriously, and Zoom has been engaged in security enhancements to continually improve its products. Zoom for Government was proud to be re-authorized for FedRAMP certification in both 2020 and 2021.

Thank you again for allowing us to provide you with our concerns about disclosure of the Security Package outside of the standard disclosure procedure. Zoom deeply appreciates your continued partnership through the FedRAMP certification process. Please do not hesitate to contact me if I can be of further assistance in this matter.

Sincerely,

A handwritten signature in black ink that reads "Lauren E. Belive". The signature is fluid and cursive.

Lauren Belive
Head of US Government Relations



**Office of Congressional and
Intergovernmental Affairs**

June 30, 2021

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

Thank you for your letter dated May 12, 2021, requesting a copy of the Zoom for Government security package. Your inquiry has been forwarded to me for response.

The U.S. General Services Administration (GSA) and the Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO) take very seriously the responsibility to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the Federal Government. The FedRAMP process establishes standard security requirements for the authorization and ongoing cybersecurity of cloud services in accordance with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130, and National Institute of Standards and Technology (NIST) guidelines. As part of this process, cloud service providers are required to deliver periodic security reports to all agency customers providing transparency into the security posture of the cloud environment. Through participation in FedRAMP, Zoom has been actively engaged in ongoing security enhancements to continually improve its Zoom for Government offering. As a result, agencies have continued to authorize and use Zoom for Government since 2019.

The security package you have requested contains highly sensitive proprietary and other confidential information relating to the security associated with the Zoom for Government product. Safeguarding this information is critical to maintaining the integrity of the offering and any government data it hosts. The FedRAMP PMO has a robust set of internal controls surrounding access to the secure repository where this information resides. This includes limiting access to individuals with authority to grant FISMA authorizations when the purpose is to grant a security authorization. Based on our review, GSA believes that disclosure of the Zoom security package would create significant security risks.

In addition, GSA solicited Zoom's views regarding your request. As per the enclosed letter, Zoom confirmed the sensitivity of the material in question and expressed significant concerns with the potential release of the information. GSA's consistent practice with regard to sensitive security and trade secret information is to withhold the


U.S. General Services Administration
1800 F Street NW
Washington DC 20405-0002
www.gsa.gov

material absent an official written request of a congressional committee with jurisdiction, and pursuant to controls on further dissemination or publication of the information. Accordingly, GSA is unable to provide you with the security package you requested at this time.

GSA values its relationship with Congress and prioritizes ensuring that we provide Congress with appropriate information about its programs and operations. To this end, GSA is happy to continue to work with you and your staff on finding ways to provide you with information about FedRAMP policies and practices.

If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

DocuSigned by:

F593809E5235492...

Gianelle E. Rivera
Associate Administrator

Enclosure