



**One Hundred Seventeenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515**

March 26, 2021

Kevin B. Thompson
Former Chief Executive Officer
SolarWinds Corporation
c/o John A. Merrigan, Esq.
DLA Piper
500 Eighth Street, N.W.
Washington, D.C. 20004

Dear Mr. Thompson:

I am writing to thank you for appearing before the Committee on Oversight and Reform and the Committee on Homeland Security at the hearing entitled “Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and the Ongoing Campaign” on Friday, February 26, 2021. Your testimony was extremely helpful in refining the Committee’s understanding of the issue. I appreciate the effort you took to prepare and present your testimony.

While many questions were asked during the hearing, the Committee has additional questions for you. Please forward your responses to the Committee clerk, Geremiah Lofton, at geremiah.lofton@mail.house.gov, by no later than Friday, April 9, 2021.

Once again, thank you for your appearance before the Committee.

Sincerely,

A handwritten signature in blue ink that reads "Bennie G. Thompson".

BENNIE G. THOMPSON
Chairman

Question for the Record from Rep. Dina Titus, a Representative in Congress from the State of Nevada

1. Nevada was one of the many state governments impacted by the SolarWinds breach. As you may know, Nevada operates on a federated IT system. Due to this federated IT system, SolarWinds did not keep records of the connections between the state-level, individual agencies that bought the company's software. This caused issues for the state's cybersecurity team when they started addressing the hack because SolarWinds's records could not recognize that each of these agencies were all housed within the State of Nevada. This meant it took longer for the cybersecurity employees to identify all the potential breaches because they had to ask each agency individually if they used SolarWinds software. How will SolarWinds ensure that, in the future, it can effectively and quickly address data breaches for state governments with federated IT systems?

Question for the Record from Rep. Michael Guest, a Representative in Congress from the State of Mississippi

1. With growing concern that users are not sufficiently educated in cybersecurity awareness, and recent cyber hacks as large as the SolarWinds which could cost up to \$100B to remedy and as small as a \$300,000 ransomware attack targeted at a school in my district in Mississippi, are you making suggestions to your employers and/or customers on best practices for security awareness and preventative measures?