DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004
www.dlapiper.com

August 5, 2021
VIA E-MAIL

The Honorable Mark Warner
Chairman
Senate Select Committee on Intelligence
703 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Marco Rubio
Vice Chairman
Senate Select Committee on Intelligence
284 Russell Senate Office Building
Washington, D.C. 20510

Dear Chairman Warner and Vice Chairman Rubio,

Thank you for the questions for the record from the Senate Select Committee on Intelligence related to the hearing on February 23, 2021 titled "Hearing on the Hack of U.S. Networks by a Foreign Adversary."

We write on behalf of our client, SolarWinds Corporation ("SolarWinds"), in response to your letter dated April 1, 2021 addressed to Sudhakar Ramakrishna. The enclosed attachment contains SolarWinds' written responses to the Committee's questions for the record on behalf of Mr. Ramakrishna.

Best regards,

John Merrigan

John Merrigan/s

Steve Phillips

Steve Phillips/s

APPENDIX A

Questions for the Record from Chairman Mark Warner and Vice Chairman Marco Rubio, Senators in Congress from the State of Virginia and the State of Florida

1. *Have you determined how the cyber actors gained access to your network? If so, please explain your findings. If not, please explain what factors are impeding your progress in making such a determination.*

   Our third-party forensic investigation firms Crowdstrike and KPMG have assessed that one of the following three vectors likely may have been leveraged by the threat actor(s) as their initial access point:

   - Third party zero-day exploitation
   - Brute force attack on external facing authentication platforms such as VPN
   - Credential compromise via phishing or watering hole attack

   Our third-party forensic investigation firms identified unauthorized access as early as January 2019, but could not identify which of the three above vectors was the initial access method by the threat actor(s) or if any earlier unauthorized access occurred due to the lack of available data dating back to that timeframe.

   While we don't know precisely when or how the threat actor first gained access to our environment, our investigations have uncovered evidence that the threat actor compromised credentials and conducted research and surveillance in furtherance of its objectives through persistent access to our software development environment and internal systems, including our Microsoft Office 365 environment, as early as January 2019.

Questions for the Record from Senator Ron Wyden, a Senator from the State of Oregon

According to a Frequently Asked Questions document published by SolarWinds, the following releases of your Orion product contained the backdoor: 2019.4 Hotfix 5, 2020.2 and 2020.2 Hotfix 1.

1. *Of these versions of your software containing the backdoor, please identify which versions SolarWinds were submitted for testing for Common Criteria certification and for potential placement on the Department of Defense Information Network (DoDIN) Approved Products List (APL).*

   The three product versions of Orion that were found to contain the backdoor, SUNBURST, were not submitted for testing for the Common Criteria certification or DoDIN APL. Prior

versions of Orion were submitted and approved. Evaluations can take up to a year, therefore only some versions go through the process. The SolarWinds Orion Suite for Federal Government must first go through Common Criteria and then is evaluated for DoDIN. SolarWinds Orion Suite for Federal Government version 3.0 completed the evaluation for common criteria and DoDIN APL. SolarWinds Orion Suite for Federal Government version 4.1 is currently under evaluation for Common Criteria.

2. *What were the results of these assessments?*

   See response above for #1.

3. *If these versions were not tested, had they been tested in a manner similar to that used to test prior versions of SolarWinds' software, do you expect that the backdoor would have been discovered? If so, please identify the specific part of the testing process that would have likely resulted in the discovery of the backdoor.*

   We do not believe that the backdoor would have been discovered in the compromised product versions if they had been tested via the Common Criteria certification as this certification only involves "Evaluation Assurance Level 2+" (EAL2+), which does not cover a deep penetration level of testing.

   For DoDIN inspection, we provide the product and DoDIN performs the testing. The detailed test plans are not known to us; therefore, we cannot determine if SUNBURST would have been discovered.

4. *When was SolarWinds first contacted by the FBI? What did the FBI tell your company?*

   SolarWinds' Vice President of Security Architecture was first contacted by the FBI via telephone on December 11, 2020, with notification of an issue about which the Company would be informed at a later time. Later that evening, the FBI sent SolarWinds a *Request for Preservation of Records* via facsimile to SolarWinds' general facsimile line. The request was to preserve for a period of ninety (90) days any and all records and other evidence related to what is now known as the cyber attack.

5. *Since the initial notification by the FBI, how much information has SolarWinds provided to the FBI, and in turn, how much information has the FBI provided SolarWinds? Is SolarWinds satisfied with the amount of information the FBI has shared with it?*

   On December 14, 2020, SolarWinds contacted FBI Cyber Division Assistant Director, Frankland M. Gorham, to provide an update on the cyber attack and to ask for assistance in the investigation. On December 15th, 2020, FBI Cyber Division leadership introduced the

SolarWinds investigation team to the FBI team leading the investigation from the Houston and San Francisco field offices.

SolarWinds is committed to transparency in its engagement with the FBI. SolarWinds has provided terabytes of unique records of information to the FBI, including but not limited to documents, log files, server images, software code, backups, and virtual hard disks. SolarWinds also participates in weekly telephone calls with the FBI and regularly invites its third-party forensic investigative firms to provide briefings to the FBI regarding developments concerning its investigation of the cyber attack.

To date, SolarWinds has received very little information from the FBI to aid in SolarWinds' efforts regarding the cyber attack. SolarWinds respects the confidentiality obligations of the FBI concerning data in its possession, but wishes more information could have been provided (if it existed) such that the company may have been able to conduct a more efficient investigation and work more closely with the government to focus remediation efforts on the customers more likely to be targeted.