DLA Piper LLP (US)
677 Broadway, Suite 1205
Albany, New York 12207-2996
www.dlapiper.com

April 6, 2021
VIA E-MAIL

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
United States House of Representatives
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairwoman Maloney,

Thank you for the questions for the record from the Committee on Oversight and Reform related to the hearing on February 26, 2021 titled "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign."

We write on behalf of our client, SolarWinds Corporation ("SolarWinds"), in response to your letters dated March 23, 2021 addressed to Sudhakar Ramakrishna and Kevin Thompson. The enclosed attachment contains SolarWinds' written responses to the Committee's questions for the record on behalf of Sudhakar Ramakrishna and Kevin Thompson.

Best regards,

John Merrigan

John Merrigan/s

Steve Phillips

Steve Phillips/s

cc: The Honorable James Comer, Ranking Member

APPENDIX A

Questions from Chairwoman Carolyn B. Maloney

1. *Please provide the Committees any final or interim reports prepared by SolarWinds or any third-party consultants or auditors engaged by SolarWinds, including but not limited to CrowdStrike and KPMG, during an investigation into the breach.*

   The Company respectfully advises the Committee that the investigations into the cyber incident are ongoing. The Company does not anticipate receiving any interim reports beyond the investigative updates that the Company is already providing periodically. Given the multiple terabytes of data that the Company is reviewing, as well as the high operational security of the threat actor, the Company does not have certainty as to whether or when a final investigative update will be completed, but the Company is endeavoring to accomplish its review by mid-May. The Company is publishing – through its public reports, blog posts and other public statements – the findings from its investigations and the learnings that the Company is applying within its own environment.

   Below are links to several investigative update blogs. The second blog is from the Company's security consultant and provides additional detailed information about the cyber incident.

   - **Findings From Our Ongoing Investigations (Blog)**
     https://orangematter.solarwinds.com/2021/02/03/findings-from-our-ongoing-investigations/

   - **Detailed CrowdStrike post authorized by SolarWinds (Blog)**
     https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

   - **New Findings From Our Investigation of Sunburst (Blog)**
     https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

   - **A Message to Our Customers (Vlog)**
     https://orangematter.solarwinds.com/2020/12/18/a-message-to-our-customers/

   - **Update on Security Vulnerability (Blog)**
     https://orangematter.solarwinds.com/2020/12/17/solarwinds-update-on-security-vulnerability/

2. *After Palo Alto Networks contacted your company in October to raise concerns about the Orion product based on behavior that they had observed—which is now believed to be*

related to the SolarWinds cyberattack—what steps did you take to investigate this issue? Why did these steps not reveal the breach of the build server at that time?

The Company respectfully advises the Committee that upon receiving an inquiry from Palo Alto Networks, the Company initiated a review and investigation pursuant to its corporate Incident Response Plan. This review and investigation were conducted by professionals from the Company's information security and engineering teams. In the course of its review and investigation, the Company requested additional information from Palo Alto Networks, but the Company was informed at that time that additional information was unavailable. Due to the complexity and sophistication of the attack, the Company was not able to identify the cause of the concerns that Palo Alto Networks identified at that time, nor did it identify the existence of Sunburst in its Orion product. Because of this, the inquiry was not escalated beyond the IT team, which meant that management and directors were not aware of the issue until December 2020. To date, the Company has not confirmed the existence of Sunburst in the Orion product deployed at Palo Alto Networks.

3. *Do you have any additional information about how the attackers gained initial access to SolarWinds' build server? If not, when do you expect to have this information?*

   The Company respectfully advises the Committee that the investigations into how the attacker gained initial access to the Company's environment are ongoing. The Company, together with third-party security experts, are reviewing multiple terabytes of data in connection with this investigation. Given the high operational security of the threat actor, as well as the passage of time since initial access, the Company does not currently know when, or if, a determination will be made as to initial access.

4. *What steps does your company still need to take to remediate this breach? How much time will remediation take?*

   The Company respectfully advises the Committee that the Company released remediations for the Sunburst code across all three affected versions of its Orion Software Platform in December 2020. The Company's investigations have not identified the Sunburst code in any of its numerous other products.

   Further, the Company has and continues to apply its learning from the attack to help protect the Company and other companies against similar attacks in the future. These "Secure by Design" initiatives from the Company are principally focused on: (1) making the Company's internal environment more secure; (2) making development of Company products more secure; (3) making the products the Company delivers more secure. The Company has and continues to make public its "Secure by Design" initiatives to help other companies apply the Company's learnings within their own environments. Examples of such publications include:

   - **Secure by Design: Securing the Supply Chain (Webcast)** https://orangematter.solarwinds.com/2021/03/31/secure-by-design-securing-the-supply-chain/

- **Secure by Design: Securing the Software Development Build (TechPod)**
  https://orangematter.solarwinds.com/2021/03/24/secure-by-design-software-development-build-techpod-38/

- **Secure by Design: Securing the Software Development Build Environment (Webcast)**
  https://orangematter.solarwinds.com/2021/03/22/secure-by-design-securing-software-development-build-environment/

- **Secure by Design: A SolarWinds Update for National Defenders (Webcast)**
  https://orangematter.solarwinds.com/2021/03/17/secure-by-design-a-solarwinds-update-for-national-defenders/

- **Secure by Design: Helping Our Customers Get Back to Business (TechPod)**
  https://orangematter.solarwinds.com/2021/03/09/secure-by-design-customers-back-business-techpod-37/

- **Secure by Design: Getting Our Customers Back to Business (Webcast)**
  https://orangematter.solarwinds.com/2021/03/05/secure-by-design-getting-our-customers-back-to-business/

- **Lessons Learned from a Cyberattack: A Conversation with SolarWinds (Webcast)**
  https://www.csis.org/events/lessons-learned-cyberattack-conversation-solarwinds-part-1-2

- **Secure by Design: Our Plan for a Safer SolarWinds and Customer Community (TechPod)**
  https://orangematter.solarwinds.com/2021/02/17/secure-by-design-our-plan-for-a-safer-solarwinds-and-customer-community-techpod-036/

- **Secure by Design: Our Plan for a Safer SolarWinds and Customer Community Webcast**
  https://orangematter.solarwinds.com/2021/02/05/secure-by-design-our-plan-for-a-safer-solarwinds-and-customer-community/

- **Continuing Our Journey to Becoming Secure by Design (Blog)**
  https://orangematter.solarwinds.com/2021/02/03/continuing-our-journey-to-becoming-secure-by-design/

- **Our Plan for a Safer SolarWinds and Customer Community (Blog)** https://orangematter.solarwinds.com/2021/01/07/our-plan-for-a-safer-solarwinds-and-customer-community/

5. *Please provide a breakdown of your expected costs associated with this breach.*

   The Company respectfully advises the Committee that, as of March 1, 2021, the Company had incurred $3.5 million of expenses related to the cyber incident through December 31, 2021. Expenses include costs to investigate and remediate the cyber incident, legal and other professional services expenses related thereto, and the cost of third-party consulting services being provided to customers at no charge. The Company also reported that it expects the costs of its "Secure by Design" initiatives to be approximately $20-25 million annually. At this time, the Company is unable to estimate with reasonable certainty the total amount of costs that will be incurred as a result of the cyber incident.

Questions from Congressman Jim Cooper:

During the House Committee on Oversight and Reform hearing on February 26, 2021, on the role of your companies in the "SolarWinds breach," I asked each of you about your company's errors and omissions insurance. Only Mr. Smith said that Microsoft was self-insured.

In SolarWinds' IPO Prospectus from 2018, SolarWinds stated, "[d]espite our security measures, unauthorized access to, or security breaches of, our software or systems could result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation and other liabilities." SolarWinds continued, "… [o]ur errors and omissions insurance coverage covering certain security and privacy damages and claim expenses may not be sufficient to compensate for all liabilities we incur."

As SolarWinds warned investors, E&O insurance could help protect the company from hacks or attacks, but might not be able to do so completely, and such coverage does nothing for your customers. There are several ways that insurance could affect your company: 1) it protects you, not your customers, so it is not necessarily aligned with your customers' interests; 2) it creates a moral hazard for your company that diminishes your interest in securing your own software, particularly if your insurance coverage is extensive; and 3) it means that future premium increases could increase your company's attention on securing your software from hacks.

When I asked each of you for information regarding your insurance coverage related to security breaches, you stated that you would need to find the answers and submit them for the record. Again, I am asking you each the following questions:

1. *If your company has errors and omissions insurance coverage for damages incurred from security breaches, or other cyber liability insurance for costs related to security breaches, please provide:*

    a. *What claims is your company making to your insurers related to the SolarWinds breach?*

        The Company respectfully advises the Committee that the Company has submitted claims under its "Cyberfirst" insurance policy and a secondary excess insurance policy for both expenses incurred and potential liabilities arising out of the cyber incident.

    b. *How much money was paid, or is expected to be paid, by your insurers for these claims?*

        The Company respectfully advises the Committee that, as of April 6, 2021, the Company has received approximately $1.8 million under its cyber insurance policy.

    c. *Since filing these claims, will your insurance premiums increase, or do you expect them to increase? If so, by how much?*

The Company respectfully advises the Committee that the amount of any increase or decrease in insurance premiums is influenced by a wide variety of factors, many of which are outside the control of the Company. At this time, the Company is unable to estimate with any reasonable certainty whether and to what extent its insurance premiums may increase in the future. The Company notes that the trend in premiums within the overall cyber insurance market has generally been increasing over time.

2. *Which insurance companies provide your errors and omission insurance, or other insurance related to security breaches? If you are self-insured, is there an internal mechanism in your company that serves the same function?*

   The Company respectfully advises the Committee that the Company's cyber insurers include Travelers Property Casualty Co. of America and Ascot Specialty Insurance Company.

3. *What are the major insurance companies that provide this coverage to your industry?*

   The Company respectfully advises the Committee that the Company is not aware of all the major insurance companies that have historically or may in the future provide cyber-related insurance coverage to the software industry. The extent and manner in which insurance companies participate in any particular insurance market vary over time, and the Company relies on its insurance brokers to help the Company obtain insurance across the various insurance markets.

4. *What percentage of your industry has this coverage? To your knowledge, do your competitors have this coverage?*

   The Company respectfully advises the Committee that the Company does not have knowledge as to the percentage of the software industry that has cyber insurance or the extent to which the Company's competitors have this coverage.