Responses to Questions for the Record from Brad Smith, President, Microsoft Corporation

House Committee on Oversight & Reform and the House Committee on Homeland Security

"*Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign*"

February 26, 2021

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?

One of the most important lessons of the SolarWinds incident is the need for greater awareness of security hygiene. Underscoring security basics must be a national priority.

The private sector plays an important role in driving awareness, educating customers about how to enhance their security posture, and enabling migration to newer and better technologies. For example, we periodically eliminate outdated technologies because of the need to migrate to newer and more secure versions of technology, including implementation of new security standards. Our services such as Microsoft Secure Score and Azure Secure Score also enable customers to visualize and assess their security posture and identify potential improvements with a comprehensive set of security controls and recommendations.

Also, about a year ago, Microsoft introduced "Security Defaults," a set of baseline recommended security settings (such as requiring all users and admins to register for Multi Factor Authentication) enabled by default in all newly-created tenants to ensure that all organizations have a basic level of security enabled at no extra cost. We also advocate that our customers adopt a Zero Trust approach to the security of their networks, including the implementation of "least privileged access" principles – all of which assumes successful compromise, but defends in depth by making it hard for an attacker to gain access to any valuable resources or data on the network.

The government also has a role to play here, through stronger risk management practices that require critical infrastructures, agencies, and others to track their risk acceptance or encourage migration to the latest approaches, in order to help close weaknesses in implementation. We absolutely have a role in making our technology as secure as possible, but we cannot force people to adopt it, and that's where implementation has a major role – as was the case here.

2. Given the demand for cyber capabilities will continue to grow at a rapid rate, can you address the current shortfalls in the workforce and provide your ideas and opportunities to meet workforce and training demands?

There are a number of things that private and public sector can do to help meet the demand for cyber professionals:

- **Increase investments in K-12 computer science education and teacher training.** Expanding access to K-12 computer science education is critical to laying a foundation for cybersecurity, and a diverse cyber workforce. Less than half of US high schools offer a computer science course and the gap is particularly pronounced for rural students and students of color. Investing in

teachers so they are trained in teaching computer science and cybersecurity is a key part of building the cyber workforce pipeline.

- **Increase federal investment in training pathways and credentials in cyber security fields and increase the diversity of the cyber talent pool.** Government can increase investments in community college/ industry partnership and apprenticeships that support individuals to gain cyber skills training. Such investments should pay particular attention to reaching and recruiting individuals from diverse backgrounds and our nation's veterans, through dedicated partnerships with and investment in HBCUs, MSIs, and other institutions.
- **Expand or create programs to encourage more industry talent into government.** Government agencies at all levels face challenges in keeping abreast of the latest developments in cybersecurity. Policymakers should consider programs to encourage graduates of accredited cyber educational degrees to teach and train state and local government entities, or rotational programs could encourage private sector talent to spend time in local, state and government. The CyberCorps Scholarship for Service could also be expanded to include more universities and post-program government positions or to create new scholarships for service pathways to attract and train K-12 teachers and be made more flexible to increase placements in state and local government.
- **Work with the private sector to develop more real-time information about cyber labor force and in-demand skills.** The National Defense Authorization Act for FY2021 requires NIST and DOD to identify multiple career pathways for cybersecurity roles. Greater information from private and public sector sources can provide key insights about the nature of cybersecurity workforce gaps and how to best build a diverse talent pipeline.

Microsoft has been doing its part to try to address these issues. For example, on K-12 computer science, we continue to expand the Technology Education and Literacy in Schools (TEALS) Microsoft Philanthropies program, which places technology industry volunteers into classrooms at over 500 high schools each year to team-teach computer science at high schools not currently offering a computer science course. We will be expanding this program in coming years to reach even more underserved areas, including in Jackson, Mississippi; Atlanta, Georgia; and Birmingham, Alabama. And with respect to cyber skills for the current workforce, we have been providing free online cybersecurity education and offering low-cost industry-recognized certifications through a global skills initiative, which offers free access to more than 500 online courses on LinkedIn Learning and Microsoft Learn containing more than 950 hours of content for in-demand roles through December 31, 2021.