



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

May 9, 2024

Mr. Brad Smith
Vice Chair and President
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Dear Mr. Smith:

We write to request your appearance before the House Committee on Homeland Security to testify at a public hearing entitled, “*A Cascade of Security Failures: Assessing Microsoft Corporation’s Cybersecurity Shortfalls and the Implications for Homeland Security.*” The hearing will take place on Wednesday, May 22, 2024, at 10:00 a.m. EDT in 310 Cannon House Office Building. The hearing will provide an opportunity for Microsoft to present its perspective on the U.S. Department of Homeland Security Cyber Safety Review Board’s (CSRB) recent report, “*Review of the Microsoft Online Exchange Incident from Summer 2023.*”¹ Specifically, the hearing will examine Microsoft’s views regarding the company’s security shortcomings,² challenges encountered in preventing significant cyber intrusions by suspected nation-state threat actors,³ and plans to strengthen security measures moving forward.⁴

As a trusted provider of operating systems, cloud platforms, and productivity software for U.S. government agencies, including those within the U.S. intelligence community, Microsoft bears a profound responsibility to prioritize and implement effective cybersecurity measures.⁵ However, the CSRB report revealed that Microsoft has repeatedly failed to prevent substantial cyber intrusions, causing grave implications for the security and integrity of U.S. government data, networks, and information,⁶ and putting Americans—including U.S. government officials—at risk.⁷ The CSRB’s report further revealed that a “cascade of Microsoft’s avoidable errors” may have allowed the 2023 Microsoft Exchange Online cyber intrusion by the People’s Republic of

¹ Cyber Safety Review Board Report, Cybersecurity and Infrastructure Security Agency, “*Review of the Microsoft Online Exchange Incident from Summer 2023*” (March 20, 2024), https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

² *Id.*

³ Microsoft Corp., “*Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*” (Jan. 19, 2024), <https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/>.

⁴ Microsoft Corp., “*A new world of security: Microsoft’s Secure Future Initiative*” (November 2, 2023), <https://blogs.microsoft.com/on-the-issues/2023/11/02/secure-future-initiative-sfi-cybersecurity-cyberattacks/>.

⁵ Microsoft Corp., “*Microsoft/Dell enter into transformative agreement with the US Intelligence Community for Microsoft Cloud Services for Government*” (May 16, 2018), <https://blogs.microsoft.com/blog/2018/05/16/microsoft-dell-enter-into-transformative-agreement-with-the-us-intelligence-community-for-microsoft-cloud-services-for-government/>.

⁶ Ellen Nakashima and Joseph Menn, “*Microsoft faulted for ‘cascade’ of failures in Chinese hack*” (April 2, 2024), Wash. Post, <https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/>.

⁷ Ellen Nakashima, et al., “*Chinese hackers breach email of Commerce Secretary Raimondo and State Department officials*”, Wash. Post, July 14, 2023, <https://www.washingtonpost.com/national-security/2023/07/12/microsoft-hack-china/>.

Mr. Brad Smith

May 9, 2024

Page 2

China (PRC) cyber espionage group, Storm-0558,⁸ to succeed.⁹ These findings underscore the critical importance of immediate and decisive action.

It is concerning enough that Storm-0558 was able to compromise the email accounts of 22 enterprise organizations and over 500 individuals globally,¹⁰ including U.S. government agencies and officials who work on national security matters relating to the PRC.¹¹ Equally alarming, however, is that Microsoft recently disclosed that its corporate email accounts were breached and compromised by “Midnight Blizzard,”¹² the very same Russian state-sponsored cyber espionage group that facilitated the 2020 SolarWinds Orion supply chain cyberattack.¹³ Following the Midnight Blizzard security breach, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive to all affected U.S. government agencies requiring them to change any logins that were compromised and investigate what else might be at risk.¹⁴ These are just two of many examples of cyber intrusions in recent years affecting certain U.S. government agencies, due to Microsoft’s cybersecurity negligence.

These cyber intrusions not only undermine public confidence in Microsoft’s ability to safeguard its operating systems, cloud platforms, and productivity software, but also raise serious questions about an apparent lack of accountability and oversight. It is imperative that Microsoft, which accounts for nearly 85 percent of the market share in the U.S. government’s productivity software,¹⁵ be held to the same level of accountability as the rest of the U.S. government’s trusted vendors.

The Committee is encouraged by Microsoft’s recent statements that it will address its security culture, which the CSRB described as, “inadequate and requir[ing] an overhaul”.¹⁶ These include launching the *Secure Future Initiative* in November 2023, which purports to “[improve] the built-in security of [Microsoft’s] products and platforms,”¹⁷ and stated commitment to “making security our top priority at Microsoft, above all else.”¹⁸ Likewise, the Committee appreciates Microsoft’s full cooperation in the CSRB investigation, which produced helpful findings and recommendations. However, given your response to other significant cyber events, such as the 2020 SolarWinds attack, we remain seriously concerned about how Microsoft follows through on its stated commitments. We simply cannot allow more nefarious cyber threat actors—including those from hostile nation-states—to compromise U.S. government data, networks, and

⁸ Microsoft Corp., “*Analysis of Storm-0558 techniques for unauthorized email access*” (July 14, 2023), <https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/>.

⁹ *Id.* at 6.

¹⁰ *Id.* at 6.

¹¹ *Id.* at 7.

¹² *Id.* at 3.

¹³ Joseph Menn, “*More companies expected to disclose email hacks by Russian intelligence*” (Jan. 26, 2024), Wash. Post, <https://www.washingtonpost.com/technology/2024/01/26/russia-hacks-sec-disclosures/>.

¹⁴ Emergency Dir. 24-02, Cybersecurity and Infrastructure Security Agency, “*ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*” (April 2, 2024), <https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system>.

¹⁵ Computer & Communications Industry Association, “*New Study Shows Microsoft Holds 85% Market Share in U.S. Public Sector Productivity Software*” (September 21, 2021), <https://ccianet.org/news/2021/09/new-study-shows-microsoft-holds-85-market-share-in-u-s-public-sector-productivity-software/>.

¹⁶ *Id.* at 1.

¹⁷ Microsoft Corp., “*Security above all else—expanding Microsoft’s Secure Future Initiative*” (May 3, 2024), <https://www.microsoft.com/en-us/security/blog/2024/05/03/security-above-all-else-expanding-microsofts-secure-future-initiative/>.

¹⁸ *Id.*

Mr. Brad Smith

May 9, 2024

Page 3

information through the exploitation of vulnerabilities in Microsoft's software, platforms, and services.

Given the gravity of the issues discussed above and the need for thorough examination and oversight, it is critical that you appear before the Committee. Your cooperation and transparency in this matter will not only assist our Committee in fulfilling its cybersecurity oversight responsibilities, but also demonstrate Microsoft's commitment to addressing cybersecurity challenges in a collaborative and proactive manner.

To confirm your appearance and ask any related follow-up questions, please contact Eric Heighberger with the Committee on Homeland Security Majority Staff at (202) 226-8417.

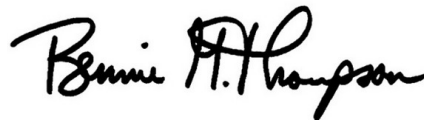
Per Rule X of the U.S. House of Representatives, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security."

Thank you for your attention to this important matter and your prompt reply.

Sincerely,



MARK E. GREEN, M.D.
Chairman
Committee on Homeland Security



BENNIE G. THOMPSON
Ranking Member
Committee on Homeland Security