COMMITTEE ON HOMELAND SECURITY
Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Ranking Member Bennie G. Thompson (D-MS)

A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security

June 13, 2024

I would like to thank the Chairman for holding today's hearing on the Cyber Safety Review Board's (CSRB) investigation of an intrusion into Federal networks involving Microsoft. At the outset, I want to make clear: this is not a "gotcha" hearing. It is not the Committee's goal to shame, embarrass, or discredit the witness, Microsoft, or any other entity mentioned in the CSRB report.

We have three objectives today: accountability, securing Federal networks, and securing the broader internet ecosystem.

Last year, we were disturbed to learn that a state-sponsored threat actor from China had accessed the e-mail accounts of high-ranking officials at the Departments of State and Commerce and an e-mail account of a Member of Congress, among others.

As the investigation unfolded, we learned that the threat actor accessed these accounts by forging tokens using a stolen signing key from 2016 and that the State Department – not Microsoft – had discovered the intrusion. By August, Secretary Mayorkas announced that the CSRB would review the Microsoft Exchange Online intrusion and the malicious targeting of cloud environments.

The CSRB engaged in a thorough and expeditious review, and its report was released earlier this year. The CSRB did exactly the kind of review it was supposed to do, and it did so in a manner only the government can. The CSRB examined a serious incident and made pointed findings and recommendations that will ultimately improve how Microsoft, other cloud service providers, and the government approach security.

It is incumbent on this Committee to hold Microsoft – one of the Federal government's most prominent IT vendors and security partners – accountable for the findings and recommendations in the report.

Microsoft deserves credit for cooperating with the Board's investigation. But make no mistake: It is Congress's expectation that Microsoft – or any similarly situated company – would do so. Microsoft's is one of the largest technology suppliers in the world, and its products are used by governments and private sector entities alike. The company provides an estimated 85 percent of the productivity software used by the Federal government. Microsoft also sells security tools and is one of the government's top cloud service providers. Moreover, a reported 25 to 30 percent of its government revenue comes from non-competitive contracts, at least in part due to the terms of its licensing agreements.

Any company with such a significant footprint in our Federal networks **has an obligation** to cooperate with a government review of how a Chinese threat actor accessed sensitive information by exploiting vulnerabilities in one of their products.

Turning to the report's findings: The CSRB determined that last summer's intrusion was "preventable and never should have occurred." Additionally, it found that "Microsoft's security culture was inadequate and requires an overhaul." As someone responsible for overseeing the security of Federal networks that rely heavily on Microsoft, and as a user of Microsoft products myself, I find these observations deeply troubling. The CSRB report

exhaustively describes how last summer's incident occurred and includes a thorough history of the threat actor's previous activities.

Importantly, the report observed that the security community has been tracking the threat actor for over 20 years. Over that time, the threat actor has demonstrated tactics and objectives like those we saw in last summer's attack. Dating back to Operation Aurora in 2009 and the R.S.A. compromise in 2011, the threat actor has a well-documented interest compromising cloud identity systems, stealing signing keys, and forging tokens that would enable access to targeted customer accounts. For over a decade, every technology provider in the world has been on notice and should have stepped-up their approach to securing identity and authentication accordingly.

But the CSRB found Microsoft did not do so. And while Microsoft did cooperate with the CSRB investigation, the Board found the company was slow to be fully transparent with the public, most notably about how the threat actor obtained the signing key. To this day, we still do not know how the threat actor accessed the signing key. Microsoft's explanations about why the key was still active in 2023 and why it worked for both consumer and enterprise accounts have not been comforting. And I remain troubled that Microsoft was reluctant to be transparent with the public that it was not confident about the root cause of the incident.

My concerns about whether we can rely on Microsoft to be transparent were heightened this morning when I read a ProPublica article about how an employee alerted Microsoft leadership to a vulnerability in its Active Directory Federation Services before security researchers publicly reported it in 2017. That vulnerability – which Microsoft chose not to fix – was ultimately used by Russian hackers to carry out secondary phases of the SolarWinds attack in 2020.

Even more troubling, the article recounts Microsoft's testimony before the Senate in 2021, which denied that any Microsoft vulnerability was exploited in SolarWinds. Transparency is the foundation of trust, and Microsoft needs to be more transparent.

In 2002, Bill Gates said "When we face a choice between adding features and resolving security issues, we need to choose security." The CSRB found that Microsoft had "drifted away from this ethos." I agree.

Last November, Microsoft announced the Secure Future Initiative, touting a re-invigored approach to security. But in January, Microsoft itself was compromised by Russian threat actors who used unsophisticated tactics to access the emails of high-level employees. Unfortunately, those emails included correspondence with government officials and put the security of Federal networks at risk once again. Basic cybersecurity tools – that were not enabled – would have thwarted the intrusion.

In May, following the CSRB report, Microsoft announced an expansion of the Secure Future Initiative that committed to making security the top priority. But the same month, Microsoft announced "Recall" – a new feature that takes and stores periodic snapshots of a user's computer screen, which has raised concerns among both privacy and security experts. I understand that last Friday, Microsoft modified the rollout of Recall in order to incorporate significant changes. I hope it will continue take the concerns of the security and privacy community seriously as it does so.

On a final note, I have been warned that the Committee's oversight of this incident will chill private sector cooperation with the Board in the future. That cannot – and should not – be the case. I want to put future subjects of CSRB investigations on notice: this Committee will not tolerate refusal to cooperate with legitimate investigations undertaken by the Board – particularly when Federal networks are involved.

Any efforts to obstruct CSRB investigations into cyber incidents would invite significant scrutiny from this Committee and would certainly force expedited consideration of proposals to grant the CSRB greater investigatory powers.

Microsoft is one of the Federal government's most important technology and security partners. But we cannot afford to allow the importance of that relationship to enable complacency or interfere with our oversight. National security demands that technology providers continue the evolution toward transparency so we can better secure the digital ecosystem. With that, I look forward to a productive conversation today about how Microsoft will work to improve its security culture, and thereby the security of its customers.

# # #

Media contact: Adam Comis at 202-225-9978