Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel [redacted]
Fax [redacted]
www.microsoft.com

Microsoft

May 9, 2022

Via Email
Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: **Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure**
Release No. 34-94382; File No. S7-09-22

Dear Secretary Countryman:

Microsoft Corporation ("Microsoft," "we," or "our") is providing this letter in response to the Securities and Exchange Commission's (the "SEC" or the "Commission") proposed rule, Cyber Risk Management, Strategy, Governance, and Incident Disclosure (the "Release" or the "Proposal").

Microsoft supports the Commission's broad objective of enhancing and standardizing disclosure regarding cybersecurity incidents, risk management, and governance. The many benefits of information technology's accelerating adoption into company operations come with inherent risks that are the rightful concern of investors. Because of the unique nature of the interconnected technology ecosystem, however, these particular areas of concern, above perhaps any other, demand careful consideration of a broad range of interdependencies and prioritization of efforts to protect the security of our national and global digital ecosystems. As a result, we believe there should be a clear, consistent framework and obligation for private sector organizations to collaborate with the government and other stakeholders when they are impacted by significant cybersecurity incidents. We see appropriate transparency and information sharing as essential to the protection of not just Microsoft's security environment but also to strengthen coordinated efforts among the broader security community. We believe public disclosure to investors through SEC filings should be structured in a manner consistent with these broader objectives. Correspondingly, we believe it is imperative – for national security interests and, ultimately, for the investing public's interests – for any rule to be closely coordinated and harmonized with other laws and regulations governing cybersecurity incident reporting and information sharing. We encourage the SEC to work closely with other interested government agencies to establish a unified approach to incident response reporting and disclosure and to achieve shared objectives and priorities.

I. Item 1.05 of Form 8-K

The SEC has proposed adding a new Item 1.05 to Form 8-K. Item 1.05 would require a registrant to provide disclosure within four business days of determining it has experienced a material cybersecurity incident.

Although we understand the Commission's desire to maintain consistency with its established four-business day window for current reporting of events covered by Form 8-K, we urge it again to consider certain unique characteristics of cyber events in how the four-business day window will apply. The Commission should explicitly allow issuers to manage the timing of a Form 8-K filing, even after a materiality determination, when compelling conditions exist such that premature disclosure would result in greater harm to the company, its investors, or the national digital ecosystem.

Risk of providing inaccurate, incomplete, or misleading information during dynamic and ongoing evaluations of cybersecurity incidents

Discovery that a cybersecurity incident has occurred initiates a complex and dynamic forensic process to analyze and understand the nature of the attack and attacker, to understand the type of data that might be affected, to assess any operational impact, and to rapidly deploy any potentially mitigating defenses. When this work starts, there is often very little detailed information available. An incident investigation and response effort can last for several months; understanding of it will evolve over that time, and threat actor behavior can change significantly throughout the course of an incident. Modern threat actor behavior also often involves a complex attack chain to overcome current cybersecurity best practices. These attack chains may involve supply chain or third-party compromise, social engineering, or insider assisted components. Many investigations are dependent on the collection and analysis of forensic data that may reside outside the boundary of the affected party. As facts are gathered and analyzed, early Form 8-K disclosures made in good faith and based on the best available information may turn out to have been incorrect. Therefore, even when a company may be able to determine a cyber incident is material relatively early in the investigation and response process, an early-stage Form 8-K could contain information that proves to be inaccurate, incomplete, or misleading. Allowing for investigations to be more well-developed before a Form 8-K is filed would result in more accurate and more decision-useful information for investors.

Risk of alerting a hostile threat actor

Due to their inherently adversarial nature, cybersecurity incidents are unlike any other item for which Form 8-K disclosure is mandated. Hostile threat actors can include criminal networks and nation states who are sophisticated enough to attack multiple organizations simultaneously and react quickly to new information. While an incident is ongoing, the threat actor may still be active in the registrant's compromised

environment. Even after a company has remediated an incident, the threat actor may still be similarly exploiting other companies, entities, or government agencies. If Form 8-K disclosure were to alert the threat actor before the incident is remediated, then the registrant or others continuing to be simultaneously impacted by a widespread attack may face increased risks different from the initial incident. For example, the threat actor could leverage alternative tactics or additional exploits to more effectively mask intrusions, plant "false flag" information, destroy indicators of compromise, accelerate data exfiltration, disrupt data integrity, or cause additional harm to the registrant or others across the ecosystem. Further, even if a threat actor has not already compromised multiple organizations, being made aware that its activity has been identified at one company could result in a threat actor accelerating its use of tactics or exploits across the entire digital ecosystem, before other targeted parties could prepare defenses (e.g., before patches for vulnerabilities could be made available or widely implemented), or a before coordinated response with cybersecurity agencies or law enforcement could be established.

As noted in Presidential Policy Directive 41 ("PPD-41"), "certain cyber incidents that have significant impacts on an entity, our national security, or the broader economy require a unique approach to response efforts. These significant cybersecurity incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors." Coordinated responses across multiple government agencies, at the international, federal, state, and local level, and involving several companies could be disrupted and undermined by premature public disclosure, making the digital ecosystem less safe. Companies may also be less willing to share information about cyber incidents if they believe it could result in another company incurring a Form 8-K disclosure obligation that would undermine response efforts.

Principles-based Form 8-K disclosure; law enforcement exception

For these reasons, we believe the SEC should consider alternatives to the four-business day reporting period. We recommend the SEC adopt a principles-based Form 8-K disclosure requirement, allowing management to exercise discretion and, as appropriate, coordination with cybersecurity, national security, and law enforcement authorities regarding the appropriate timing of filing the Form 8-K.

If the Commission decides to adopt a four-business day reporting period (or other set reporting period), we believe that the rule must allow for an exception when the registrant is informed by a cybersecurity, national security, or law enforcement agency that a delay of disclosure would serve national security interests or would allow law enforcement to more effectively disrupt or pursue apprehension of the perpetrator.

II. Definitions

"Cybersecurity Incidents"

The proposed rule defines "cybersecurity incident" as:

> An unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

We do not believe that an incident that "jeopardizes" a registrant's information systems or information residing therein is an appropriate mandatory Form 8-K disclosure trigger. The Release notes that this definition is derived from PPD-41 and other comparable sources. We believe a key distinction between the objectives or purposes of many of those referenced sources, on the one hand, and SEC reporting, on the other , is that the former sources contemplate *confidential* reporting to support a law enforcement or national security response. The goal of such confidential reporting and agency response, among other things, is to prevent harm before it occurs. In those circumstances, real time confidential reporting when systems or information are *jeopardized* is appropriate and necessary.

In contrast, we do not believe the same rationale exists for real time Form 8-K disclosure regarding cybersecurity incidents. While an incident may create significant risk of harm – *i.e.*, it may jeopardize a registrant's information systems or information — it may not result in harm because a threat actor could be contained, or a vulnerability patched before there is any material impact to the company.

Just as Form 8-K does not mandate disclosure of potential material agreements or potential bankruptcies, we do not believe Form 8-K should mandate disclosure of an event that may never materially impact the company. We recommend that the SEC revise this definition so that Form 8-K disclosure is required where there is actual impact – *i.e.*, disclosure should be required only if the company is materially affected by a cybersecurity incident.

III. Disclosure of Cybersecurity Incidents That Have Become Material in the Aggregate

The Release creates a requirement to provide disclosure "when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate". The Release notes that registrants should "analyze related cybersecurity incidents for materiality." It does not, however, define what constitutes a "series", what it means to be "related", or what time-period should be assessed. If this requirement is adopted, we believe additional clarity around these terms should be provided. Even if

additional clarity were provided, we believe this requirement would present significant challenges for companies and be of limited value to investors.

A materiality analysis involves considerations that are different from the analysis conducted to scope, respond to, and remediate an incident. Performing an in-depth materiality analysis of a single significant cybersecurity incident is a fact-intensive and time-consuming process, involving many internal and potentially external constituencies. The Proposal would create an ongoing materiality analysis requirement for every obviously immaterial, even trivial, cybersecurity incident that is arguably part of a series. There would be both significant practical challenges for some companies and limited value in the case of others.

First, a company would have to assess every cybersecurity incident in enough detail to determine whether it "related" to others or was part of a "series." That alone could be a difficult, if not impossible, exercise for some organizations, in part because of the challenge of attribution. Where companies own information resources, they may not have sufficient expertise or resources to focus on tracking threat actors or otherwise determining whether incidents are related, instead prioritizing defensive, remediation, and response activities. Where registrants use information resources owned by others, they may be dependent on context from their providers, which may or may not focus resources on tracking threat actors or whether incidents are otherwise related. Furthering the challenge is that each incident may potentially be part of more than one series.

Second, each incident that is determined to be part of a series would have to be evaluated to determine its significance and impact so the company could aggregate it into the overall materiality analysis. That would involve a detailed assessment by business, financial, cybersecurity, and legal resources for incidents that are clearly immaterial.

Third, the analysis for each incident in the series would have to be stitched together into an overall materiality analysis for each series. The overall analysis effort would be ongoing and have to track each incident as it evolves. That would require the gathering and monitoring of facts at a level that is unwarranted for immaterial events, which is in tension with the materiality threshold in the Proposal.

The complexity and layered nature of these analyses would render any resulting disclosure of questionable value. Simultaneously, it would open the door for potential second-guessing around how a company analyzed any group of events. Microsoft recommends not including this requirement in the final rule.

IV. Cyber Expertise

The proposed rule amends Item 407 of Regulation S-K to require disclosure regarding board members' cyber expertise. This requirement is a significant expansion of Regulation S-K's Item 401(e)'s existing disclosure obligation for companies to "discuss the specific experience, qualifications, attributes or skills that led to the conclusion that the person should serve as a director for the registrant." Although the proposed disclosure creates no explicit obligation to have a "cyber expert" on a company's board, it does create implicit pressure to do so. The rule as proposed invites investors and other stakeholders to question boards with no or minimal cyber expertise among their members as to whether they are equipped to oversee cybersecurity risk.

We are concerned that this trend of requiring disclosure of specific expertise will lead to boards being made up of specialists who will lack an overall picture of the business landscape. The best boards are comprised of highly accomplished generalists with deep intellect and acute critical thinking skills. As a board of directors strives to maintain a diverse set of experiences and attributes, it also expects that each member will be able to understand and contribute meaningfully to the oversight of the broad range of material business, risk, and regulatory issues their role requires them to oversee. Management's responsibility includes educating and communicating to the board in a way that enables effective oversight around these issues. As a result, specific areas of substantive expertise may be beneficial but not required among board members. No board should unduly rely on an "expert;" rather, it should ensure management, or the board's own outside resources, bridge any gaps and answer any questions until the board is satisfied that it, collectively, can effectively discharge its oversight duties.

V. Conclusion

We appreciate the opportunity to provide input on the Proposal. If there are any questions regarding our comments or recommendations, we would welcome the opportunity to discuss them with you. Thank you for your consideration.

Sincerely,

/s/ Keith R. Dolliver

Keith R. Dolliver
Vice President and Deputy General Counsel
Microsoft Corporation