Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

June 5, 2023

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

**Re: Microsoft's Comment on Proposed SEC Cybersecurity Rules – (1) Regulation SCI (S7-07-23); (2) Proposed Rule 10 (S7-06-23); and (3) Regulation S-P (S7-05-23)**

Dear Ms. Countryman:

Thank you for the opportunity to comment on the above-referenced proposed cybersecurity rules (collectively, the "**Proposed Rules**"). Microsoft appreciates the SEC's public engagement. Because the Proposed Rules' terms concerning cybersecurity incident reporting periods present common issues, we are submitting a consolidated letter in each of the rulemaking dockets. And as noted below, our comment also addresses three issues unique to the proposed changes to Regulation SCI.

Many covered entities use our cloud services, which may make Microsoft a service provider under the Proposed Rules. In addition, Microsoft has significant experience with identifying and protecting against cybersecurity risks and threats and responding to cybersecurity incidents. We are supportive of the SEC's efforts to maintain fair and orderly markets through stronger cybersecurity and operational resilience, and we offer our recommendations in furtherance of this objective.

**1. The SEC should use a 72-hour cyber incident reporting period, instead of shorter periods, to harmonize the Proposed Rules with other federal incident reporting requirements.**

The Proposed Rules include cybersecurity incident notification time periods that range from "immediately" to "48 hours." These different periods apply to incident notification from service providers to their covered entity customers, initial notice from a covered entity to the SEC, written notification to the SEC using prescribed forms, supplemental notification based on discovery of material new information, and final reports upon the conclusion of an incident or investigation. *See* Proposed Rule SCI, 17 C.F.R. § 242.1002(b); Proposed Rule 10, 17 C.F.R. § 242.10(c)(1), (2); Proposed Regulation S-P 17 C.F.R. § 248.30(b)(5)(1).[1] Notably, the cost-benefit analyses of the Proposed Rules do not identify why a 48-hour or shorter reporting period is optimal.

[1] The SEC's recently proposed changes to the Investment Advisers, Registered Investment Rule (S7-04-22) also include proposed 48-hour incident reporting periods. *See* 17 C.F.R. Parts 275.204-6 (Proposed Rule 204-6). The principles and points we raise in this Comment apply to those proposed rule changes as well.

We urge the SEC to use, for all provisions listed above, a 72-hour reporting deadline. Specifically, where the SEC determines that a cybersecurity incident reporting requirement is appropriate, the applicable rule should provide that the entity with the notification responsibility shall provide the required notice to the recipient as soon as possible but no later than 72 hours. The reporting deadline should begin to run once the entity with notification responsibilities has a reasonable basis to conclude that a notifiable incident has occurred or is occurring.

Use of this 72-hour reporting deadline throughout the Proposed Rules has multiple advantages. First, it will align the SEC's rules with other notification requirements that may apply to entities covered by the Proposed Rules, significantly reducing complexity and compliance burdens for covered entities and their service providers. Each of the following authorities, among others use a 72-hour reporting deadline: the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), Pub. L. No. 117-103, 136 Stat. 49 (2022); Executive Order 14028, "Improving the Nation's Cybersecurity," 86 Fed. Reg. 26,633 (May 12, 2021), directing the federal government to incorporate a 72-hour reporting period into the Federal Acquisition Regulation ("FAR"); the Defense Federal Acquisition Regulation Supplement ("DFARS"), 48 C.F.R. §§ 204.7302(b) and 252.204-7012(c); the New York State Department of Financial Services' ("NYDFS") Cybersecurity Requirements for Financial Service Companies, 23 NYCRR § 500.17(a); the European Union's General Data Protection Regulation ("GDPR"), Regulation (EU) 2016/679; and Article 23 of the EU's new Network and Information Security Directive ("NIS 2 Directive"), Directive (EU) 2022/2555. Many covered entities under the Proposed Rules and their service providers will be critical infrastructure operators under CIRCIA, are government contractors subject to the FAR and DFARS, are covered entities under NYDFS regulations, and conduct business in Europe, meaning that they will be required to comply simultaneously with the Proposed Rules and these other requirements.

Second, using a 72-hour reporting deadline will further the White House and Congress's express policy of harmonizing cyber incident reporting requirements. Under CIRCIA, Congress expressed a clear preference for harmonization of federal incident reporting requirements, including by directing the interagency Cyber Incident Reporting Council to "coordinate, deconflict, and harmonize Federal incident reporting requirements," *see* § 2224(a), 136 Stat. at 1054. The recently published White House National Cybersecurity Strategy also emphasizes the need to harmonize regulations to reduce compliance burdens, noting that "[e]ffective regulation minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets." White House National Cybersecurity Strategy at 9. The SEC also has recognized this policy goal, as its Release for the Proposed Rules notes the importance of consistency with industry standards for addressing cybersecurity risk. *See* 88 Fed. Reg. 20,212, 20,263 fn. 410 (Apr. 5, 2023).

Third, a consistent 72-hour reporting deadline promotes more effective cyber security incident response and cyber threat information sharing compared to shorter and varied reporting periods. A primary goal of incident reporting requirements is to promote awareness and information sharing among persons or organizations affected by an incident or in a position to help mitigate potential threats. Thus, accurate, complete, and actionable information is critical. Immediately after the discovery of a cybersecurity incident, key information about the incident, such as cause, methods, scope, and impact, often are unknown. Premature reporting according to a 48-hour or shorter

deadline, in our experience, increases the likelihood of reporting inaccurate or incomplete information, which is of little-to-no value and tends to create confusion and uncertainty.

**2. Regulation SCI should not require reporting of "*significant attempted*" intrusions because there is no set of clear, objective, and consistent criteria for identifying a significant attempt.**

In the proposed changes to Regulation SCI, the definition of "System Intrusion" would expand to include *significant attempted intrusions.* Specifically, the proposed definition would require SCI entities to report "[s]ignificant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria." Proposed Rule SCI 242.1000. Significantly, the proposed changes to Regulation SCI do not define what constitutes a "significant attempted authorized entry," but rather would require covered entities to articulate these criteria for themselves with ad hoc, subjective, and disparate criteria "as determined by the SCI entity." Regulation SCI would provide no standard definition creating a potentially unworkable and administrable situation for cloud service providers like Microsoft that serve many SCI entities.

Identification of events that qualify as "significant attempted" intrusions will consume considerable resources, result in confusing and inconsistent reporting, and yield little discernable benefit. Although the Release identifies considerations that could guide creation of organization-specific criteria, including the presence of a "known threat actor," "reconnaissance," or a "targeted campaign," these considerations are too vague to make this requirement workable. *See* 88 Fed. Reg. 23,146, 23,185 (Apr. 15, 2023). Where an intrusion has been attempted but is unsuccessful, organizations often will have far too little intelligence about the attack to evaluate these criteria. Organizations will needlessly devote energy to analyzing events that do not warrant reporting resulting in overreporting, which can drown out important information about bona fide cyber threats.

Further, the proposed requirement to report attempts is inconsistent with CIRCIA, which limits notifiable incidents to those that *actually* jeopardize information or systems. *See* § 2240(6)(B), 136 Stat. 1039. Additionally, the Financial Stability Board (FSB) has reported that near misses, defined as an event where no harm or impact occurs but has the potential to do so, should be excluded from reporting requirements. *See* Achieving Greater Convergence in Cyber Incident Reporting: Overview of responses to the consultation (fsb.org) *at page 3.* Directing organizations to develop criteria for identifying attempts and correspondingly requiring them to invest further resources in assessing whether "attempts" should be reported will divert scarce resources away from security operations.

**3. Regulation SCI should not require industry-wide analyses of service provider market concentration risk.**

The SEC's proposed changes for Regulation SCI include a requirement for each SCI entity to conduct a risk assessment of third-party provider concentration among SCI entities or within the relevant industry ("**Risk Assessment**"). *See* Proposed Rule 1001(a)(2)(ix).

Microsoft supports the proposed requirement that an institution assess concentration risk within the institution itself, *i.e.*, its reliance on a particular provider with assessments of business continuity and

exit planning, is appropriate so long as such requirements are technology neutral and not focused exclusively on cloud computing. Assessment of concentration risk within a particular organization is not a new concept but, rather, one that institutions have been grappling to address in legacy on-premises environments for some time.

But as proposed, the Risk Assessment requirement extends beyond an individual institution to include an industry-wide assessment and therefore appears unworkable. Such an assessment is more expansive than what an SCI entity itself realistically can assess or manage. An individual SCI entity likely will not have market information showing third-party provider concentration at a macro level.

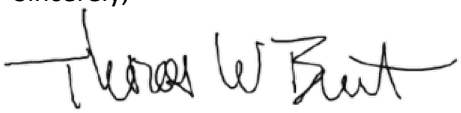
**4. Regulation SCI should permit pooled penetration testing among SCI entities.**

Proposed changes to Regulation SCI also would require each SCI entity to conduct annual penetration testing. *See* Proposed Rule 1000 (defining "SCI review"). Microsoft supports penetration testing to maintain strong security and recommends one change to improve this requirement.

Because SCI entities may rely on common service providers, the rule should expressly permit SCI entities to participate in coordinated, pooled penetration testing so that the testing may be performed efficiently at scale and applicable to multiple different SCI entities. Pooled testing should be subject to safeguards, such as direction by one SCI entity, reasonable limits on pool size to maintain high level of testing, and consistent with testing under the Regulation and NIST standards.

Thank you again for the opportunity to comment on the Proposed Rules. We look forward to continuing working with the SEC, other agencies, and our customers to enhance security.

Sincerely,



Thomas W. Burt
Corporate Vice President, Customer Security & Trust
Microsoft Corporation