SANDBOXAQ™

May 6, 2022

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549-1090

RE: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure; File No. S7-09-22

Dear Ms. Countryman,

SB Technology, Inc. ("we" or "SandboxAQ") welcomes the opportunity to comment on the Security and Exchange Commission's (the *"Commission")* proposed rule establishing a framework for disclosure regarding cybersecurity risk management, governance and incident reporting by public companies subject to the reporting requirements of the Securities Exchange Act of 1934 (the "Cybersecurity Proposal").[1] We appreciate the Commission's interest in enhancing and standardizing disclosure regarding cybersecurity risks in order to provide transparency for investors.

Background of SandboxAQ

SandboxAQ is an enterprise SaaS company developing commercial solutions at the nexus of quantum technology and artificial intelligence ("AI"). We focus on quantum-resistant cryptography, or post-quantum cryptography ("PQC"), quantum sensing, quantum simulation and quantum communications and work closely with commercial and public sector stakeholders to identify and develop solutions to quantum-related opportunities and threats. Our work and collaboration with stakeholders have broad implications for the government, computer security, telecom, financial services, healthcare, aerospace, defense, transportation and other data-intensive sectors. Our core focus and capabilities include the following:

- *Cybersecurity* – Protecting large enterprises against quantum-related threats from independent or state-sponsored adversaries targeting RSA-encrypted data, information, networks, infrastructure, communications and more.
- *Quantum Sensing* – Leveraging quantum magnetometry and AI to detect previously undetectable stimuli, leading to breakthroughs in navigation, detection, imaging and other use cases that could enhance our global leadership and strengthen national security.

[1] U.S. Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Securities Exchange Act Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22 (March 9, 2022) (the "*Proposing Release*").

- *Quantum Simulation* – Digitally simulating quantum interactions at the molecular level, which will collapse the research and development time and cost for drug discovery, product design, prototyping and development, materials science and other broad use cases.
- *Quantum Communications* - Designing next generation hardware leveraging properties of quantum mechanics and entanglement to enable secure, long-distance, end-to-end transmission of quantum data and information across a large collection of quantum computers and sensors.

Through collaboration with the federal government, we have shaped the adoption of "zero trust" principles and approaches ("Zero Trust") for securing federal information systems and networks. Zero Trust is an approach to cybersecurity that secures an organization's information networks by rejecting the assumption that users within such networks should be implicitly trusted. Rather, under Zero Trust, digital interactions are validated at every stage. Zero Trust is designed to protect modern environments and enable digital transformation by enforcing strict authentication methods, leveraging network segmentation, limiting internal lateral movement, providing layer 7 threat prevention, and simplifying granular, "least access" security policies.[2] The federal Zero Trust initiative runs under the authority of the Federal CIO Council, a forum of federal Chief Information Officers, and the National Institute of Standards and Technology (the "NIST") is a partner in the effort, leading research and technical work with volunteers from other federal agencies. The comments and suggested amendments to the Cybersecurity Proposal set forth below are informed by the Zero Trust Cybersecurity Principles released by the U.S. Office of Management and Budget on January 26, 2022.[3]

PQC refers to methods of data and digital communication encryption that are resistant to cyberattacks by quantum computers, which pose a serious threat to many of the cryptographic algorithms (particularly public-key cryptography) that are currently widely used to protect digital information. By developing new kinds of cryptographic approaches that can be implemented using modern classical computers, PQC helps ensure that organizations and their networks will be protected against future attacks from quantum computers, particularly as such computing power becomes increasingly common.[4]

Key Recommendations for Cybersecurity Proposal

In principle, we support the Commission's efforts to bolster disclosure of cybersecurity risk management, strategy, governance and incident reporting, particularly in light of the rapidly evolving threats that cybersecurity incidents pose to public companies and capital markets. In the following sections, we suggest amendments that build upon the proposed disclosure regime and endeavor to further protect investors by providing them with more fulsome, standardized information regarding companies' cybersecurity risk management practices and risk profiles. Specifically, the Commission should (1) require registrants to provide additional disclosure on prospective risk mitigation efforts, including the use or planned use of PQC in response to growing quantum computing threats, (2) incorporate forward-looking elements, such as access to continuing education, into the list of criteria used to determine board

[2] Scott Rose, Oliver Borchert, Stu Mitchell & Sean Connelly, *Zero Trust Architecture, NIST Special Publication 800-207* (August 2020), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[3] U.S. Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022), available at https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[4] For more information on PQC, *see* National Institute of Standards and Technology, *Post-Quantum Cryptography*, available at https://csrc.nist.gov/projects/post-quantum-cryptography.

expertise in cybersecurity and (3) further standardize the terms and standards used to inform investors of companies' cybersecurity risk profiles.

1. **Registrants should provide additional prospective disclosure on their cybersecurity risk management and mitigation plans, including disclosure of PQC-related practices.**

One of the principal goals of the Cybersecurity Proposal is to provide investors with a more meaningful, comprehensive understanding of the "growing cybersecurity risks registrants are facing," so that they may properly value companies' securities and make well-informed investment decisions that allocate capital efficiently.[5] As the threat posed to commonly-used data encryption and protection methods by quantum computing continues to grow and evolve, investors would benefit from more detailed disclosure regarding registrants' prospective risk mitigation measures, including whether companies have implemented or plan to implement PQC to protect data and digital infrastructure from future cybersecurity attacks. Accordingly, and in response to the Commission's request for comment on whether the new Item 106(b) of Regulation S-K should be adopted as proposed, SandboxAQ recommends supplementing the language of Item 106(b)(1)(iv) to solicit additional information on the PQC-related measures that registrants have taken to "prevent, detect, and minimize effects of cybersecurity incidents."[6] Such amended Item 106(b)(1)(iv) should thus read, "The registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents, and if so, provide a description of the types of activities undertaken and identify whether such activities include methods of quantum-resistant encryption of post-quantum cryptography."

Although this disclosure obligation could yield a number of valuable responses, examples of the types of information solicited might include:

- whether registrants have created a cryptographic inventory to know what cryptography is used in their infrastructure;
- whether companies' encryption is currently in compliance with quantum-resistant algorithms and technology, as defined by the NIST;
- whether registrants maintain complete inventories of systems using non-compliant encryption;
- whether registrants have a timeline to transition systems using non-complaint encryption to begin using compliant encryption; and
- whether registrants maintain a complete inventory of every device authorized and operated for official business.

Such information would enhance understanding of companies' susceptibility to future cybersecurity incidents, allowing investors to better evaluate how cybersecurity-related costs could impact the value of such companies' securities and thus make better informed investment decisions. The resulting reduction in information asymmetry between investors and registrants could in turn augment the positive indirect and spillover effects of the Cybersecurity Proposal already highlighted by the Commission.[7] For example, if companies respond to this obligation by adopting measures to implement PQC and protect themselves against quantum-related threats, their vulnerability to future cyber-attacks and the likelihood of resulting negative externalities would be reduced. In turn, this could have the positive effect of accelerating the

[5] Proposing Release at 53.
[6] Proposing Release at 106.
[7] Proposing Release at 82.

already-likely replacement of current cryptographic protocols with PQC, which is particularly important for applications with long-term security requirements or especially sensitive data. Additionally, the mere disclosure of a cybersecurity risk mitigation plan commensurate with the risk level of secured information could have the secondary effect of deterring bad actors from future cybersecurity attacks.

Disclosure of cybersecurity risk management through PQC implementation and migration plans, as well as enhanced disclosure on any known role of quantum threats in material cybersecurity incidents, could also be incorporated into the new Item 1.05 of Form 8-K. As currently proposed, Item 1.05 focuses largely on backward-looking disclosure involving material cybersecurity incidents, including information on the timing, scope and effects of such an incident and any present efforts to remediate the incident.[8] In response to the Commission's request for comment on whether Item 1.05 should require any additional information about a material cybersecurity incident, SandboxAQ suggests that registrants reporting a material incident should also disclose whether their efforts to mitigate or remedy the incident involve use or implementation of PQC. Such a disclosure obligation could be imposed by amending the proposed Item 1.05(a)(5) to read, "whether the registrant has remediated or is currently remediating the incident, and if so, whether such remedial measures include methods of quantum-resistant encryption of post-quantum cryptography." Further, Item 1.05 should require that registrants disclose any imminent threats to electronic information – particularly high-risk information, such as healthcare or financial data – resulting from a material cybersecurity incident known to stem from quantum computing. Such information would provide investors with a better understanding of the post-incident risk profile of registrants, as well as the likelihood of extended harmful impacts from the incident.

2. Companies should consider whether directors undergo continuing cybersecurity education in determining whether they have "expertise" in the field.

The Commission also requests comment on whether the proposed amendments to Item 407 of Regulation S-K should be modified to require additional information with respect to board members' expertise in cybersecurity.[9] While we believe the changes to Item 407 set forth in the Cybersecurity Proposal take an important step towards recognizing and solidifying the crucial role that board leadership plays in shaping companies' approach to cybersecurity risk management and mitigation, we suggest adding more forward-looking elements to the list of criteria that registrants are prompted to consider when determining the portion of their board with cybersecurity expertise.

As proposed, the factors to be considered in establishing expertise are uniformly backward-looking and include prior work experience, certifications or degrees and other background knowledge and skills.[10] This approach fails to account for the fact that cybersecurity expertise is a dynamic, evolving body of knowledge and that leadership must remain informed of new threats and technologies, such as PQC and related quantum capabilities, to adequately manage and oversee companies' cybersecurity programs and responses. SandboxAQ recommends remedying this gap by adding, "and whether the director participates in continuing education programs related to cybersecurity" to the factors listed in the proposed Item 407(j)(1)(i).[11] Such addition would help ensure that any director disclosed as having

---

8 Proposing Release at 21.

9 Proposing Release at 46.

10 Proposing Release at 45.

11 Proposing Release at 110.

cybersecurity expertise maintains a current, well-informed understanding of trends in cybersecurity risk management. In turn, this would provide investors with a more meaningful understanding of the caliber of board cybersecurity oversight and allow them to make better informed investment and director voting decisions.

3. **Disclosure required by the Cybersecurity Proposal should be further standardized through utilization of NIST definitions and frameworks.**

We support the Commission's stated objective of standardizing cybersecurity disclosure to facilitate the comparison of such disclosure across companies for investors.[12] However, the Cybersecurity Proposal would benefit from further standardization through consistent use of definitions and frameworks established by the NIST. For example, in response to the Commission's request for comment on whether defining "cybersecurity" in the proposed Item 106(a) of Regulation S-K would be helpful for investors and registrants, SandboxAQ supports providing a defined term and further suggests relying upon the definition set forth by the NIST: "prevention of damage to, protection of, and restoration of computers, electronic communications systems, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[13] As a term foundational to the understanding and implementation of the Cybersecurity Proposal, cybersecurity should be defined so as to clarify for registrants the scope of their disclosure obligations and to provide investors with a baseline understanding of this complex and multifaceted concept.

Using a definition that aligns with the NIST's will also facilitate and ease compliance for registrants, as the NIST is widely recognized as a standard-setting organization at the forefront of cybersecurity expertise. Through its research and guidance, the NIST helps companies of disparate sizes and from various sectors better understand, manage and reduce their cybersecurity risk and protect their networks and data. In 2017, Executive Order No. 13800 made use of the NIST's cybersecurity framework (discussed further below) mandatory for all federal agencies, further solidifying the organization's credibility and authority.[14] Implementing the NIST definition would also be consistent with the Commission's approach to defining other terms in the Cybersecurity Proposal, such as "cybersecurity incident," "cybersecurity threat" and "information systems," which draw upon language from the NIST glossary.[15]

Along with use of the NIST definition of cybersecurity, SandboxAQ recommends that the Commission supplement the Cybersecurity Proposal with a requirement that registrants disclose whether they utilize or have a plan in place to begin utilizing the NIST's Framework for Improving Critical Infrastructure Cybersecurity (the "*NIST Framework*") in managing their cybersecurity risks.[16] Because

---

[12] Proposing Release at 11.

[13] National Institute of Standards and Technology (NIST), *Computer Security Resource Center Glossary*, available at https://csrc.nist.gov/glossary/term/cybersecurity.

[14] Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), available at https://www.govinfo.gov/content/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

[15] Proposing Release at 41.

[16] The NIST Cybersecurity Framework is a voluntary, publicly available set of standards, guidelines and practices for reducing cyber risks to critical infrastructure. It was originally developed by the NIST in collaboration with industry stakeholders upon the issuance of Executive Order No. 13636, *Improving Critical Infrastructure*

cybersecurity risk management is highly technical and rapidly-changing, investors without expertise in the field would benefit from simplified baseline disclosure rooted in the standards of a credible third party. Such disclosure would complement the more granular information provided by our proposed disclosure on PQC and quantum-related threats (which would likely prove more beneficial to sophisticated market participants) by allowing investors to easily understand and evaluate the overall quality of companies' risk management practices. Disclosure regarding use of the NIST Framework meets this investor need and imposes minimal compliance burdens for companies for several reasons, including the NIST's previously-discussed reputation as an esteemed source of third-party data and standards. Additionally, the NIST Framework is widely used by industry actors across size and sector, rendering it easily recognizable to companies complying with the new disclosure obligations. Lastly, because it is comprised of general standards and guidance that can be adapted to a particular company's size, operations and risk management needs, the NIST Framework provides the most appropriate touchstone for easily comparing cybersecurity risk profiles across industries.

****

In evaluating possible changes to the disclosure regime set forth in the Cybersecurity Proposal, we urge the Commission to maximize benefits for investors, registrants and capital markets by establishing robust and meaningful disclosure obligations. Such obligations should yield thorough information on the prospective elements of companies' cybersecurity risk preparedness, including the use of PQC and the availability of ongoing education for directors with cybersecurity expertise, and should utilize standardized terms and frameworks set forth by the NIST. We also encourage both the Commission and lawmakers to consider how requiring specific actions and cybersecurity protections, such as PQC, would supplement this valuable disclosure regarding registrants' cybersecurity infrastructure and further benefit companies, investors, markets and other stakeholders.

SandboxAQ appreciates your consideration of our comments and suggestions.

Respectfully submitted,

Valerie Vasquez

Director of Government Affairs, SandboxAQ

cc: Honorable Gary Gensler, Chair
Honorable Allison Herren Lee, Commissioner
Honorable Hester M. Peirce, Commissioner
Honorable Caroline A. Crenshaw, Commissioner
Renee Jones, Director of the Division of Corporate Finance

Cybersecurity, in 2013. The NIST's role in setting standards for cybersecurity risk management through the NIST Framework was further solidified by the Cybersecurity Enhancement Act of 2014. Use of the NIST Framework is mandatory for U.S. federal government agencies, and organizations and firms across industries have adopted its use as well. For more information on the NIST Framework, *see* National Institute of Standards and Technology, *Cybersecurity Framework*, available at https://www.nist.gov/cyberframework.