May 5, 2022

Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-0609

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

Dear Secretary Countryman,

The Biotechnology Innovation Organization (BIO) appreciates the opportunity to provide comments to the Securities and Exchange Commission's (SEC or Commission) proposed rule to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.[1]

BIO is the world's largest life sciences trade association representing nearly 1,000 biotechnology companies, academic institutions, state biotechnology centers and related organizations across the United States and in more than 30 other nations. BIO members are involved in the research and development of innovative biotechnology products that will help to solve some of society's most pressing challenges, such as managing the environmental and health risks of climate change, sustainably growing nutritious food, improving animal health, enabling manufacturing processes that reduce waste and minimize water use, and advancing the health of our families.

The biotechnology industry is instrumental in advancing society and is considered a critical technology for American economic security in the new era.[2] Accordingly, we agree that cybersecurity is *the* defining business risk of the digital age. As companies increasingly gather, analyze, and create data-derived products, cybersecurity will be central to securing core business operations and competitive moats, and ensuring that stakeholders and shareholders are adequately apprised about this rising threat.

However, BIO urges the Commission and the Administration to take a holistic approach to their regulatory agenda with a particular focus on what this recent wave of regulation means for small

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed Rule
[2] https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

companies, the diminishing incentives to become a public company, and the duplicative nature of reporting that will exist once the Administration's regulatory agenda is fully implemented.

The Commission acknowledges that small companies will be disproportionately affected by the rule without specifically noting that small companies are the least likely to be victims of cybersecurity incidents, as detailed in the same academic research the Commission uses as ballast for the economic cost of cyber incidents to markets.[3]

Summary of Concerns and Recommendations

Many companies already report cyber incidents to various federal, state, local, and international bodies. New laws enacted this year in addition to this proposed rule will dramatically increase the reporting burden for small companies. The proposed rule also threatens to put small companies at odds with law enforcement. The domestic reporting systems should be streamlined and coordinated to reduce the burden and significant costs that will be borne by small companies.

- **BIO urges the Commission to coordinate with other federal and state regulators and agencies on current and proposed reporting requirements to have a common set of information to streamline reporting.**

- **BIO urges the Commission to have agency agreements in place with CISA, FTC, and other regulatory agencies that currently require cyber incident reporting to consolidate filing.**

- **BIO urges the Commission to work with the Department of Justice to issue guidance to federal, state, and local law enforcement agencies for all parties to be aligned with the Commission's standing that federal securities law reporting requirements are distinct from cooperation with law enforcement.**

Since the intention of the proposed rule is to drive corporate behavior to implement cybersecurity programs, the Commission should take steps to help small companies mature into this reporting regime and organizational structure. Most private, venture-backed companies will not have these structures and personnel in place by the time they would naturally intend to IPO. These requirements, in addition to the other requirements the Commission has proposed and will propose, will disproportionately affect small companies with consequences for capital markets and capital formation in the United States.

[3] Supra note 133 in the proposed rule Section C: Potential Benefits and Costs of the Proposed Amendments

- **BIO urges the Commission to extend emerging growth company and smaller reporting company exemptions to include cybersecurity management and board disclosures.**

- **BIO urges the Commission and its regulatory partners to provide resources and assistance to small businesses to train executives and management to ensure an equal playing field between small and large companies.**

The Impact of Regulation on Small Business Capital Formation

At the end of every bull market comes a wave of regulation meant to curb the perceived excesses of the prior cycle. We are at a similar juncture. The current wave of public company regulation was expected given the end of Internet 2.0 era and as we transition into the new Industrial Age. There are new threats to our markets and society that require systemic approaches.

We urge the Commission to view their regulatory agenda with the hindsight of lessons learned from past waves of regulation, the consequences they had for capital formation and capital markets, and the eventual need to roll back regulations to more meaningful and more effective levels. This proposed rule will compel action which will increase the cost of capital for smaller companies and increase capital expenditure for cybersecurity service providers.

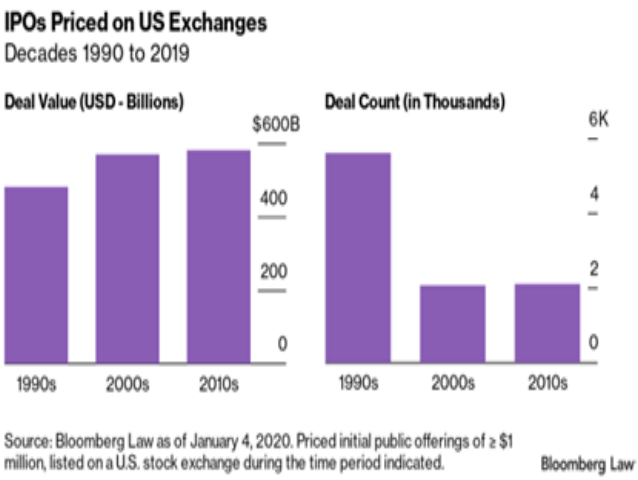
The net consequence of heavy regulatory reporting burdens for public companies are two-fold. (1) Fewer companies will join public markets, and (2) the companies that do become public will be large. Put another way, more regulation means you create larger companies.

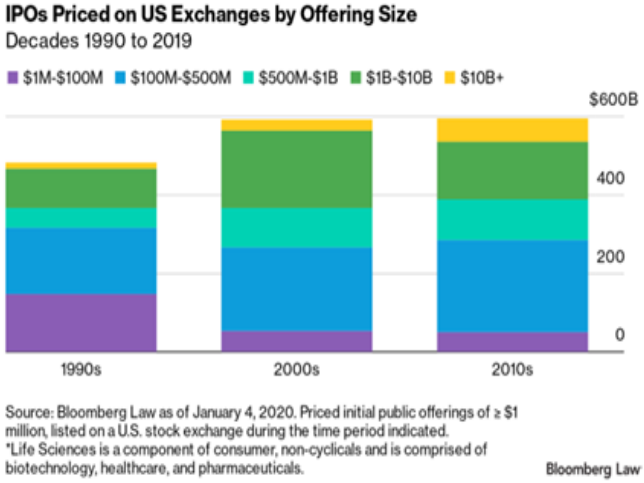
This is a natural consequence of requiring more capital to support a larger, more costly operating structure to meet the demands of regulators. This was the result of Sarbanes-Oxley. Similarly, in the wake of Dodd-Frank financial institutions and asset managers became much larger.

As the chart below illustrate, in the wake of Sarbanes-Oxley the number of IPOs fell but deal values increased. This means that fewer companies went public, but those that did tended to be large. From the 1990s to the 2000s the number of IPOs fell by more than 60 percent.[4] Another way to look at it is by breaking down the deal values by offer size where one can note that since the 1990s the number of companies seeking $1 million to $100 million collapsed.[5] Congress had to enact new legislation, most crucially the JOBS Act of 2012, to reignite the IPO market,

[4] https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-three-decades-of-ipo-deals-1990-2019
[5] Id

particularly for smaller companies. This is concerning given that the JOBS Act is no longer as bipartisan as it once was.





The current wave of regulation is threatening to do the same to capital markets and capital formation. Congress soon will have to enact new ways to incentivize going public because of the significant cost and onerous, duplicative reporting entailed with being a reporting company.

Overlapping Reporting and Lack of Law Enforcement Exemptions

As noted in the Commission's proposed rule, most domestic companies must already report to various local, state, and federal agencies and law enforcement when cybersecurity breaches occur. As the Commission duly notes, all 50 states also have their data breach laws as do the different countries in which biotechnology companies typically operate, such as the United Kingdom and the European Union.

BIO is troubled by the Commission's declaration that securities law "is distinct" from obligations to local, state, and federal law enforcement efforts to find and stymie the root cause of cybercrime. This places significant pressure on small companies, who have baseline legal counsel and often outsource more complex legal services, to dramatically increase expenditures when a cyber incident occurs as law enforcement will not take kindly to efforts to circumvent investigations while they are taking place.

The Commission should not promulgate rules that will force companies to clash with law enforcement agencies without first having the opinion and support of the Department of

Justice, who should simultaneously issue guidance to ensure that federal, state, and local law enforcement are aware of new obligations and protocols for reporting.

While many biotechnology companies do not retain patient records from clinical trials—typically held by academic institutions, healthcare centers, and clinical research organizations—the business model pivot defining the new era entails owning more data. So, biotechnology companies are increasingly having to report under the Health Insurance Portability and Accountability Act (HIPAA) and to the Federal Trade Commission (FTC) using separate reports and systems.

Many companies already implement the National Institute of Standards and Technology (NIST SP 800-53 and SP 800-137, Information Security Continuous Monitoring**)** protocols and are audited on ISO 27001 (global information security management standards) compliance. This constitutes four different reporting requirements that are currently in existence for which small biotechnologies may be accountable.

Furthermore, the President just signed into law the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which mandates that all critical infrastructure entities report to the Cybersecurity and Infrastructure Security Agency (CISA) on material cybersecurity incidents and ransomware payments. CISA has not yet promulgated any rules pursuant to the CIRCIA. Companies do not yet know which industries are included under the Act as "covered entities" reporting "cover incidents" as both definitions have not yet been defined by the Director of CISA. We can only assume that since the White House has labeled biotechnology as a critical industry and the Presidential Policy Directive 21 from 2013 named "healthcare and public health" as critical infrastructure that our industry will soon also contend with reporting to CISA.

Having to report simultaneously to four federal agencies in addition to state, local, and international regulators and law enforcement is a significant burden for small companies.

There must be more coordination and data-sharing at the federal level with data-sharing to states and localities. The Commission should establish agency agreements with CISA and have sharing mechanisms for FTC and HIPAA reporting. The Commission should also work with their law enforcement and regulatory colleagues to create standard templates for reporting to streamline the multiple reporting process.

"Naming and Shaming" and the Cost of Capital for Small Businesses

The Commission acknowledges in the proposed rule that once disclosures are mandated, companies that do not have cybersecurity programs will face a higher cost of capital. The Commission also notes in the proposed rule that the average market capitalization of domestic filers that did not make cybersecurity-related disclosures was $2.2 billion.[6]

This means that micro- and small-capitalization companies comprise the majority of registrants that did not report cybersecurity-related disclosures since $2 billion in market capitalization is the threshold for inclusion in most exchange-traded funds that track the small-cap sector. **Taken together, the SEC is saying that micro- and small-capitalization companies will face higher cost of capital once this proposed rule is implemented. These companies need exemptions when smaller reporting companies and an onramp to compliance as emerging growth companies.**

The Commission cites academic research from Kamiya et al, which suggests that an average value loss of $495 million per attack, inferred by a mean -0.84% abnormal return witnessed in the wake of cybersecurity incident announcements. However, this interpretation by the Commission does not keep with the language and intent of the study. The Commission ignored and omitted the fact that these inferred losses stemming from the observed return implies a mean company market capitalization of $58.9 billion.[7]

Put another way, **cyberattacks mainly affect large companies and are <u>not</u> material for smaller companies**. This is corroborated in the same study, which the Commission omitted in its presentation, and states,

> "Our likelihood analysis shows that **firms are more likely to experience cyberattacks when they are larger**, included in the list of Fortune 500 companies, financially less constrained, more highly valued, and have more intangible assets. We also find that cyberattacks are more likely to occur in firms operating in industries that are less competitive.[8]" (emphasis ours)

[6] Id

[7] The Commission cites Kamiya et al., "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms," Journal of Financial Economics 2021 who states "*Consistent with this expectation, we find a significant mean cumulative abnormal return (CAR) of –0.84% during the three-day window around cyberattack announcements for our full sample of personal information loss.* ***With a mean market value of about $58.93 billion for our sample of attacked firms, this translates into an average value loss of $495 million per attack.***"

[8] Id

The Commission is incorrectly suggesting that the significant loss of $495 million on average per incident is systemic, which is not the case. These losses are clearly concentrated in large companies, yet this loss statistic of $495 million has been used to justify compelling sub-$2 billion companies to have the same organizational structures, board composition, and capital expenditures for cybersecurity as a $59 billion company.

The Commission also misrepresented the significance of a -0.84% cumulative three-day abnormal return following cyber incident announcements.[9] This return is *well within* the standard deviation of returns for the S&P 500 (which has a historical daily standard deviation of 0.98%) and would not be considered significant by most market participants, especially over a period of three consecutive days.[10] Furthermore, the same study cited by the Commission, Kamiya et al, found "**no consistent evidence that the stock price reaction is worse for financially constrained firms**.[11]"

Any market practitioner would expect an exogenous shock to affect small-cap company share prices more than large-cap company share prices given that small-cap companies have higher volatility. Put another way, small-cap companies have higher betas, which means for one percent move in the S&P 500 small cap companies should experience a greater than one percent move. However, the study suggests that this is not the case for cybersecurity incidents reported. Both large-cap and small-cap companies experience the same stock reaction to the same shock. This is further evidence that these rules are not germane for small companies. **Small companies should be exempt**.

BIO urges the Commission to extend emerging growth company and smaller reporting company exemptions to include cybersecurity management and board disclosures.

BIO urges the Commission to provide emerging growth companies and smaller reporting companies with training and resources to meet these new operational and reporting obligations.

[9] If a stock had a historical standard deviation of 1% and moved 0.8% on news, most market participants would suggest that the news was either not significant or the market had priced-in that news so the reaction was muted.

[10] CFA Institute

[11] Id

Responses to Key Questions

Q2c: Should we modify or eliminate any of the specified disclosure items in proposed Item 1.05?

BIO recommends removing the disclosure for "remediating" cyber incidents from Form 8K as this aspect seems to be covered in Proposed Rule Section C, Disclosure about Cybersecurity Incidents in Periodic Reports, mandating disclosure of "material changes, additions, or updates to information disclosed on Form 8K in registrants' quarterly Form 10Q or annual report Form 10K."

Registrants will effectively be responsible for filing updates via Form 8K, Form 10Q, and Form 10K for the same incident. This is a regulatory overcorrection in disclosure and reporting. While there is a current societal trend for requiring information as frequently as possible, the Commission must balance the need for ongoing reports against the cost to registrants of time and resources. The reporting of remediation can be disclosed in Form 10Q with the same level of effectiveness as filing another Form 8K between quarterly reports.

Q3: Could any of the proposed Item 1.05 disclosures or the proposed timing of the disclosures have the unintentional effect of putting registrants at additional risk of future cybersecurity incidents? If so, how could we modify the proposal to avoid this effect? For example, should registrants instead provide some of the disclosures in proposed Item 1.05 in the registrant's next periodic report? If so, which disclosures?

BIO is concerned with the amount of information that the Commission is proposing to be filed as cyber incidents are being investigated and/or remediated. To report the proposed information publicly would signal to attackers the extent of knowledge regarding the investigation as well as the planned remediation. The resources required to complete Item 1.05, as proposed, would certainly distract from a company's ability to assist law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident, as well as implementation of any mitigation efforts needed to prevent future cybersecurity incidents

Q4: We are proposing to require registrants to file an Item 1.05 Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident. Would the proposed four-business day filing deadline provide sufficient time for registrants to prepare the disclosures that would be required under proposed Item 1.05? Should we modify the timeframe in which a registrant must file a Form 8-K under proposed Item 1.05? If so, what timeframe would be more appropriate for making these disclosures?

Filing Form 8K is not a costless exercise with both internal and external costs associated with drafting and filing the form with the Commission. While the biotechnology industry is inherently a heavy user of Form 8K in reporting of clinical trial, regulatory, financing, and other corporate updates, each update can take more than the proposed four days to complete and filing costs are non-trivial, especially if a small company must file several updates via Form 8K throughout the process. The costs will add up per incident over time.

Further, as noted in the comments above and in answers further below, the biotechnology industry does not claim domain expertise in cybersecurity of information technology systems. Most biotechnology companies are small companies without the resources to carry a full-time cybersecurity expert on staff, much less at the Board or management level. Existing legal and regulatory consultants will have to fill this gap, and the market is currently not prepared to absorb this timeline. Small companies will face unknown expenditures associated with this new filing, including cybersecurity consultants.

Q5: Should there be a different triggering event for the Item 1.05 disclosure, such as the registrant's discovery that it has experienced a cybersecurity incident, even if the registrant has not yet been able to determine the materiality of the incident? If so, which information should be disclosed in Form 8-K based on a revised triggering event? Should we instead require disclosure only if the expected costs arising from a cybersecurity incident exceed a certain quantifiable threshold, *e.g.*, a percentage of the company's assets, equity, revenues or net income or alternatively a precise number? If so, what would be an appropriate threshold?

BIO contends that *all* disclosures should be rooted in the established materiality standard. Mandating disclosures that are not material to a business introduces costly obligations that may be bore in terms of the direct costs associated with filing immaterial disclosures, indirect costs due to the risks associated with disclosing nontraditional information about a company's inner working, and via the increased cost of capital that will be implied in markets due to the asymmetry of information caused, unduly, by regulatory disclosure predicated on standards other than materiality.

Quantifiable triggering mechanisms would be a welcome triggering mechanism for all companies as the materiality of financial affects from exogenous shocks are easy to understand, universally wanted by investors, and universally applicable across industries. An exogenous shock, such as a cyber incident, can be material if one percent or more of company's revenues are affected by the incident.

Q6: To what extent, if any, would the proposed Form 8-K incident reporting obligation create conflicts for a registrant with respect to other obligations of the registrant under federal or state law? How would any such conflicting obligations arise, and what mechanisms could the Commission use to ensure that registrants can comply with other laws and regulations

Generally, BIO is troubled at the volume of reporting that will have to occur across various federal, state, local, and international law enforcement and regulatory bodies for the same cybersecurity incident. BIO is also concerned with the lack of coordination between domestic federal and state agencies and law enforcement. There must be more law enforcement and regulatory coordination.

The healthcare industry is already responsible for reporting to a panoply of local, state, and federal regulators and law enforcement agencies. The reporting burden will therefore possibly include reporting to securities and health regulators as well as law enforcement in all 50 states as well as six federal agencies.

The Commission should work with its federal and state-level cybersecurity partners to ensure minimal overlap and efficient reporting mechanisms are in place prior to implementing any reporting rules. Such partnerships should define a clear chain of command in which industry is not inappropriately left to be at conflict with law enforcement or other regulators. Notably, the Commission should establish agency agreements with CISA, FTC, DoJ, and HHS at the federal level before implementing a final rule.

Q7: Should any rule provide that the Commission shall allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security?

BIO is highly concerned that the proposed rule is putting registrants on a collision course with law enforcement. The SEC should not knowingly put companies at odds with law enforcement. Accordingly, the Commission should allow for exemption in cases where the U.S. Attorney General, State Attorney General, or District Attorney requests a delay and in matters where review by law enforcement is still pending. The Commission must work with the Department of Justice in establishing reporting criteria for state and local jurisdictions to use when assessing the law enforcement implications versus the securities reporting requirements for cyber incidents.

Further, *before the proposed rule in finalized and implemented the SEC must establish* that it is has "an agency agreement and sharing mechanism" in place with the CISA to ensure that there are no duplicative reporting efforts. BIO also contends that the SEC and CISA should have agency

agreements and sharing mechanisms with the Federal Trade Commission (FTC) as the FTC already mandates certain data breaches to be reported.

The Administration should endeavor to streamline the reporting process so that the most pertinent agency is notified at the earliest opportunity, and that submission should count for all other relevant agencies and regulators.

Q10. As described further below, we are proposing to define cybersecurity incident to include an unauthorized occurrence on or through a registrant's "information systems," which is proposed to include "information resources owned or used by the registrant." Would registrants be reasonably able to obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them? Would a safe harbor for information about cybersecurity incidents affecting information resources that are used but not owned by a registrant be appropriate? If so, why, and what would be the appropriate scope of a safe harbor? What alternative disclosure requirements would provide investors with information about cybersecurity incidents and risks that affect registrants via information systems owned by third parties?

The biotechnology industry is not in the business of providing information technology or information security services. Hence most biotechnology companies outsource this critical function to service providers with expertise. Software infrastructure, utility suppliers, and other service provides should be responsible for the safety, soundness, and reporting of cyber incidents of their products and services. Biotechnology companies, as cyber risk management services customers, are not best situated to understand the nuance of a cyber incident. Biotechnology companies will base their materiality assessments on the assessments and information provided by cyber security service providers. Any delay, omission, misrepresentation, or error on behalf of the provider should not be transferred to the customer of those services and, hence, should be provided with adequate safe harbors.

Furthermore, the nature of clinical trials is for biotechnology companies to contract these critical tests out to clinical research organizations and a myriad of other service providers who handle, store, and report patient data, including genomic data. All of these service providers to the biotechnology industry have a duty to report to their customer if any such incident occurs. Customers should not be held liable for reporting breaches or for delays in receiving said reports from service providers. Customers should not have to monitor EDGAR or social media to determine if a material breach has occurred at a service provider.

The rules should include safe harbors for reporting on incidents affecting information resources that are used but not owned by a registrant for these reasons.

Q13. Should we include Item 1.05 in the Exchange Act Rules 13a-11 and 15d-11 safe harbors from public and private claims under Exchange Act Section 10(b) and Rule 10b-5 for failure to timely file a Form 8-K, as proposed?

Yes. As with any transition period, there will be a learning curve and companies should have safe harbors to reduce liability. Further, as the pace and sophistication of cyber incidents magnifies, companies should be provided with safe harbor protections when disclosing these events.

Q14. Should we include Item 1.05, as proposed, in the list of Form 8-K items where failure to timely file a Form 8-K will not result in the loss of a registrant's eligibility to file a registration statement on Form S-3 and Form SF-3?

Form S3 is instrumental for emerging biotechnology companies that have a consistent cadence for raising capital to start, adjust, and expand clinical trials. As these costs increase over time, public biotechnology companies will only accelerate their use of Form S3 for issuing new securities to raise more capital. BIO supports this safe harbor.

Q15. Should we require registrants to disclose any material changes or updates to information that would be disclosed pursuant to proposed Item 1.05 of Form 8-K in the registrant's quarterly or annual report, as proposed? Are there instances, other than to correct inaccurate or materially misleading prior disclosures, when a registrant should be required to update its report on Form 8-K or file another Form 8-K instead of providing disclosure of material changes, additions, or updates in a subsequent Form 10-Q or Form 10-K?

BIO cautions the Commission in proposing so many disclosures across different filings. BIO recommends that the Commission implement rules that consider the significant burden of repeated filings. The Commission should pick one relevant filing form for all disclosures. For instance, if the Commission believes that Form 8K strikes the perfect balance between substance and timing, then the Commission should only require registrants to file Form 8K for all matters related to cyber incidents and leave management with the option to discuss incidents in Management Discussion and Analysis sections of Form 10K.

Q16. Should we require a registrant to provide disclosure on Form 10-Q or Form 10-K when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate, as proposed? Alternatively, should we require a registrant to

provide disclosure in Form 8-K, rather than in a periodic report, as proposed, when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate?

As noted above, the Commission should pick one specific form for the reporting of cyber-related incidents.

Q17. Should we adopt Item 106(b) and (c) as proposed?

While BIO understands the need for such disclosures, the Commission is potentially exposing much of the domestic market to cyber criminals if these disclosures are required in the next proxy season. The Commission acknowledged in the proposed rule that there is a non-negligible risk that the reporting of cyber-readiness potentially exposes companies to being targeted once there is a disclosure. Given that the research cited by the Commission contends that small companies tend to not have cybersecurity capabilities, one would expect that the lack of cyber-readiness would inappropriately expose small companies to this risk as knowledge of their shortcomings becomes widely known.

Essentially, the Commission has acknowledged that this will compel companies to implement cybersecurity programs and processes. However, the Commission is not responsible for providing support or guidance. This will require small, pre-revenue companies (the majority of listed biotechnology companies) to raise new capital to comply with the Commission's new set of disclosures.

Historically, investors are less willing to provide capital to companies to implement regulatory requirements (which constitute a negative return on invested capital) rather than deploying capital to advance the company's core business interest, which in this case is advancing R&D and clinical trials.

Q19. Would defining "cybersecurity" in proposed Item 106(a) be helpful? Why or why not?

No position.

Q22. Are there concerns that certain disclosures required under Item 106 would have the potential effect of undermining a registrant's cybersecurity defense efforts or have other potentially adverse effects by highlighting a registrant's lack of policies and procedures related to cybersecurity? If so, how should we address these concerns while balancing investor need

for a sufficient description of a registrant's policies and procedures for purposes of their investment decisions?

As noted above, there is a non-negligible risk that disclosure of cybersecurity programs or consultants may have the unintended consequence of creating new cybersecurity targets, a fact made more concerning given the recent cyber incident incurred at Okta.

Q23. Should we exempt certain categories of registrants from proposed Item 106, such as smaller reporting companies, emerging growth companies, or FPIs? If so, which ones and why? How would any exemption impact investor assessments and comparisons of the cybersecurity risks of registrants? Alternatively, should we provide for scaled disclosure requirements by any of these categories of registrants, and if so, how?

As detailed in the narrative above, small companies are seldom targets of cybercriminals but will see the most severe direct and indirect costs associated with complying with the rule and increases in their costs of capital. Smaller reporting companies and emerging growth companies should be exempt from reporting of Item 6. For instance, a classic biotechnology company running clinical trials should not need to implement new management structures that focus on cybersecurity risks as the company does not host patient data and only runs experiments.

The median employee count for BIO's members is 19. This includes executives and R&D personnel, such as researchers and lab technicians. These small biotechnology companies do not have the capacity, nor the business need, to have institutional structures related to the management, planning, oversight, and maintenance of cybersecurity related systems and suppliers.

These companies should not have to hire extra employees specifically for the purposes of implementing cybersecurity related programs when their main focus for raising capital is to advance research and development of products whose intellectual property is easily searchable in patent libraries. However, a health technology company that focuses on delivering telehealth or administers decentralized clinical trials may have to report given that their entire business model is gathering, storing, and analyzing customer data.

Smaller reporting companies and emerging growth companies should be exempt from proposed Item 6.

Q24. Should we provide for delayed compliance or other transition provisions for proposed Item 106 for certain categories of registrants, such as smaller reporting companies, emerging growth companies, FPIs, or asset-backed securities issuers? Proposed Item 106(b), which

would require companies to provide disclosures regarding existing policies and procedures for the identification and management of cybersecurity incidents, would be required in annual reports. Should the proposed Item 106(b) disclosures also be required in registration statements under the Securities Act and the Exchange Act?

Smaller reporting companies and emerging growth companies should be exempt from reporting on Item 106(b), Item 106(c), and Item 407(j). At minimum, smaller reporting companies and emerging growth companies should be given a phase-in period for reporting. BIO believes this is particularly germane given that research indicates that these companies tend to not be targeted by cyber criminals.

As noted in the comments above, the current wave of regulatory reporting requirements for public companies has historically led to a decline in IPOs, particularly of small companies seeking additional capital to improve and expand operations. Given that smaller reporting companies and emerging growth companies tend to not have mature structures when they IPO, these companies should not be required to disclose proposed Item 106(b) information in registration statements. Most, if not all, of these companies will be using raised capital to form these corporate structures.

BIO remains concerned that the Administration, including the Commission, is not viewing their regulatory plan holistically. Seeking to implement significant changes to disclosure frameworks, all of which will require significant capital to implement, will stifle capital formation as companies looking to IPO will reconsider as they did in the wake of Sarbanes-Oxley (as noted above).

Q25. To what extent would disclosure under proposed Item 106 overlap with disclosure required under Item 407(h) of Regulation S-K ("Board leadership structure and role in oversight") with respect to board oversight of cybersecurity risks? To the extent there is significant overlap, should we expressly provide for the use of hyperlinks or cross-references in Item 106? Are there other approaches that would effectively decrease duplicative disclosure without being cumbersome for investors?

No position.

Q26. Would proposed Item 407(j) disclosure provide information that investors would find useful? Should it be modified in any way?

The proposed Item 407(j) is not helpful as a general regulatory disclosure. As noted above, this will asymmetrically impact smaller companies. The biotechnology industry already has tremendous

difficulty in filing board seats with those that have expertise in biotechnology, clinical trials, and in the sub-specialty of the therapeutic target of the company.

For example, finding board members that have successful track records running clinical trials and raising capital for companies in amyloid-targeting therapeutics in the treatment of Alzheimer's disease is remarkably difficult. In addition to this expertise of the therapeutic area (neurology with a focus on dementia), sector (biotechnology), and board role (audit, etc), small biotechnology companies must also work towards finding diverse candidates to fill these board-level roles in an industry that suffers a structural deficit in talent, due to nationally low participation rates in STEM education, and specifically in board-ready candidates from diverse backgrounds. Finally, with such limited pools of talent, there is significant competition and added complexity from proxies, who limit the number of boards on which a director can sit. While this may be pertinent for larger companies, it is a significant problem for smaller companies.

The Commission is adding to this complexity with the need for cybersecurity expertise. In a separate proposed rule, the Commission is compelling the same need for climate risk expertise. This is not feasible for small biotechnology companies.

As we note above and is implied in the Commission's proposed rule and citations within the proposed rule, smaller companies are not the main targets for cybercriminals. Hence, the proposed Item 407(j) seems more appropriate as a requirement for index inclusion. This is the most efficient mechanism for ensuring that larger companies have board representation for this matter. For example, S&P 500, Dow Jones Industrial Average, MSCI, Russell, Wilshire, and CRSP Indices can mandate that in order to be included in their respective index, a company must fit the market capitalization and board structure requirements.

Q27. Should we require disclosure of the names of persons with cybersecurity expertise on the board of directors, as currently proposed in Item 407(j)(1)? Would a requirement to name such persons have the unintended effect of deterring persons with this expertise from serving on a board of directors?

The cybercriminal industry prides itself on public embarrassment. There is little benefit in providing fodder to those with malicious intent.

Q28. When a registrant does not have a person with cybersecurity expertise on its board of directors, should the registrant be required to state expressly that this is the case under proposed Item 407(j)(1)? As proposed, we would not require a registrant to make such an explicit statement.

No. This serves no purpose other than naming and shaming.

Q29. Proposed Item 407(j) would require registrants to describe fully the nature of a board member's expertise in cybersecurity without mandating specific disclosures. Is there particular information that we should instead require a registrant to disclose with respect to a board member's expertise in cybersecurity?

No position.

Q31. Would the Item 407(j) disclosure requirements have the unintended effect of undermining a registrant's cybersecurity defense efforts or otherwise impose undue burdens on registrants? If so, how?

Singling out a person is never a good idea and will bring unwanted attention to a company's oversight structure. How companies handle cybersecurity at the board level need not be detailed.

Q32. Should 407(j) disclosure of board expertise be required in an annual report and proxy or information statement, as proposed?

No position.

Q33. To what extent would disclosure under proposed Item 407(j) overlap with disclosure required under Item 401(e) of Regulation S-K with respect to the business experience of directors? Are there alternative approaches that would avoid duplicative disclosure without being cumbersome for investors?

There would be significant overlap. The specific expertise attributed to cybersecurity does not need to be its own item.

Q34. As proposed, Item 407(j) does not include a definition of the term "expertise" in the context of cybersecurity. Should Item 407(j) define the term "expertise"? If so, how should we define the term?

No position.

Q35. Should certain categories of registrants, such as smaller reporting companies, emerging growth companies, or FPIs, be excluded from the proposed Item 407(j) disclosure

requirement? How would any exclusion affect the ability of investors to assess the cybersecurity risk of a registrant or compare such risk among registrants?

As noted above, smaller reporting companies and emerging growth companies should be exempt from Item 407(j) disclosure requirements. The cybersecurity risk of a registrant is not ameliorated by the presence of a cybersecurity expert on a board in the same way that clinical trial risk is not ameliorated by the presence of an expert on the board.

Q36. Should we adopt the proposed Item 407(j)(2) safe harbor to clarify that a director identified as having expertise in cybersecurity would not have any increased level of liability under the federal securities laws as a result of such identification? Are there alternatives we should consider?

If the Commission moves to implement the rule as written, there should be safe harbors as proposed in Item 407(j)(2).

Q37. As proposed, disclosure under Item 407(j) would be required in a proxy or information statement. Should we require the disclosure under Item 407(j) to appear in a registrant's proxy or information statement regardless of whether the registrant is relying on General Instruction G(3)? Is this information relevant to a security holder's decision to vote for a particular director?

No position.