ALERT MEMORANDUM

SEC Proposes New Disclosure Rules for Cybersecurity Incidents and Governance

April 4, 2022

On March 9, 2022, the U.S. Securities and Exchange Commission issued for public comment a proposal to enhance and standardize disclosure requirements related to cybersecurity incident reporting and cybersecurity risk management, strategy, and governance. The proposed rule changes would apply to domestic and foreign companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.[1]

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Helena Grannis
+1 212 225 2376
hgrannis@cgsh.com

Anthony M. Shults
+1 212 225 2693
ashults@cgsh.com

Specifically, the Commission's cybersecurity proposal would:

— amend Form 8-K to require disclosure about material cybersecurity incidents within four business days after a registrant determines that it has experienced such an incident;

— amend Forms 10-Q and 10-K to require updates to previously disclosed cybersecurity incidents, and to require disclosure of previously undisclosed immaterial cybersecurity incidents that have become material in the aggregate;

— amend Form 10-K and Form 20-F to require annual disclosure regarding a registrant's policies and procedures for identifying and managing cybersecurity risks; a registrant's cybersecurity governance, including board of director oversight of cybersecurity risks; and management's role, and relevant expertise, in assessing and managing cybersecurity risks and implementing related policies, procedures, and strategies;

— amend Item 407 of Regulation S-K to require disclosure about the cybersecurity expertise, if any, of members of the registrant's board of directors;

— amend Form 6-K to add "cybersecurity incidents" as a potential reporting topic for a foreign private issuer (FPI); and

— require the proposed disclosures to be provided in Inline XBRL, a machine-readable format for presenting financial information.

[1] The Commission's release, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Release Nos. 33-11038, 34-94382, can be found here. Commissioner Peirce, the only sitting Republican commissioner, dissented from the proposal.

In line with other recent proposals by the Commission, the public comment period is brief. Comments are due on May 9, 2022—60 days after issuance of the proposal and 47 days after its publication in the Federal Register.[2]

This Alert Memorandum describes the Commission's cybersecurity proposal and provides some general takeaways and possible issues for comment.

I. Background of the Proposal

With the growing prevalence of cyber incidents, and companies' increased reliance on secured and reliable information systems and digital connectivity, the Commission believes that it is necessary to adopt additional disclosure requirements for material cyber incidents and cybersecurity management and governance. To address this need, the Commission released a proposed rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (the "Proposal"), which will, if adopted, supplement existing guidance and provide specific requirements for registrants in this area.

The Proposal notes that costs to companies from cyber incidents and the protective measures needed to prevent them have become more extensive and potentially material, and that these costs can negatively impact stock prices and affect short- and long-term shareholder value. Further, the Commission explains that cybersecurity is a critical governance-related issue for boards and investors and notes that investors are increasingly requesting information regarding registrants' cybersecurity risk management, strategy, and governance practices.

Against this backdrop, the Commission stressed that "whether and how a registrant is managing cybersecurity risks could impact an investor's return on investment and would be decision-useful information in an investor's investment or considerations." The Commission stated that "investors would benefit from more timely and consistent disclosure about material cybersecurity incidents" and "from greater availability and comparability of disclosure by public companies across industries regarding their cybersecurity risk management, strategy and governance practices."

The Proposal builds on the 2011 guidance issued by the SEC's Division of Corporation Finance ("2011 Staff Guidance") and the 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosures issued by the Commission itself ("2018 Interpretive Release").[3] The 2011 Staff Guidance highlighted companies' potential cyber-related disclosure obligations in the context of risk factors, management's discussion and analysis of financial condition and results of operations, business description, legal proceedings, and financial statements. The 2018 Interpretive Release reinforced and expanded on the 2011 Staff Guidance, and stressed a number of factors that may inform a company's materiality determinations in the cyber context, including the range of harm that cybersecurity incidents could cause to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions related to cyber incidents.[4] The 2018 Interpretive Release also explored two key topics not addressed in the 2011

[2] The short comment period is consistent with the current Administration's push to advance final rules more quickly. Objections to such short comment periods have been raised by state bar associations, securities law practitioners, commenters, and members of Congress, especially given the increased pace of overall rulemaking.

[3] *See* CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011) ("2011 Staff Guidance"), available here; Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459, 34-82746 (Feb. 26, 2018) ("2018 Interpretive Release"), available here.

[4] The 2018 Interpretive Release suggests that, in determining their obligations to disclose cyber-related matters, companies should weigh, "among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and the impact of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations."

Staff Guidance, namely the application of insider trading prohibitions in the cybersecurity context and the importance of cybersecurity policies and procedures as key elements of enterprise-wide risk management.[5]

The new March 2022 Proposal from the Commission would codify much of the 2011 Staff Guidance and 2018 Interpretive Release, and go further in meaningful ways.

II. The Proposal

A. Disclosure by U.S. Registrants

Prompt Disclosure of Material Cybersecurity Incidents on Form 8-K

The March 2022 Proposal would amend Form 8-K to add a new Item 1.05, which would require disclosure within four business days after a registrant determines that it has experienced a material cybersecurity incident.[6] The Commission justified this proposed rule change in part due to its growing concern that material cybersecurity incidents are underreported and that existing reporting may not be sufficiently timely.[7]

New Form 8-K Item 1.05 would require registrants to disclose when the incident was discovered and whether it is ongoing; a brief description of the nature and scope of the incident; whether any data was stolen, altered, accessed, or used for any other unauthorized purpose; the effect on the registrant's operations; and whether the incident has been remediated or is being remediated.

The trigger for a required disclosure under proposed Item 1.05 is the date on which a registrant determines a cybersecurity incident is material, rather than the date of discovery of the incident. For incidents that have a significant impact on a company's central operations, the materiality determination may coincide with the date of discovery, but that is not always the case. In any event, the Commission expects "registrants to be diligent in making a materiality determination in as prompt a manner as feasible." Materiality would be governed by the familiar standard in the disclosure context—specifically, whether "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision or if it would have significantly altered the total mix of information made available." The Commission notes the need to use quantitative and qualitative factors to determine whether an incident is material in light of the specific circumstances presented, as discussed in the 2018 Interpretive Release.

The proposed rule provides a non-exclusive list of cybersecurity incidents that may, if determined to be material, trigger disclosure:

— An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the registrant's security policies or

[5] *See* Cleary Gottlieb Alert Memorandum, "SEC Issues Interpretive Release on Cybersecurity Disclosure," Feb. 28, 2018, available here.

[6] The March 2022 Proposal 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." It defines "information systems" as "information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations." The definitions of "cybersecurity incident" and "information systems" would be incorporated into the proposed rules for Form 8-K reporting and would also apply to Item 106 of Regulation S-K, discussed below.

[7] The Commission has been conducting a sweep of public companies that were reported to be affected by the cyberattack first disclosed in December 2020 involving the compromise of software made by SolarWinds Corp. The Commission requested that certain companies voluntarily provide information as to whether they were affected by the cyber incident and regarding their resulting disclosures, and also inquired about any other cyber incidents affecting the companies. *See* Cleary Gottlieb Alert Memorandum, "Cybersecurity: Data Breaches, Ransomware Attacks and Increased Regulatory Focus," Jan. 11, 2022, available here.

procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;

— An unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems;

— An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;

— An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or

— An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

A registrant is not expected to provide detailed technical information about its planned response or its systems or any potential system vulnerabilities in a way that "would impede the registrant's response or remediation of the incident."

Updating vs. Amending. The Proposal would require updates to any cybersecurity incidents previously reported on Form 8-K to be made in Quarterly Reports on Form 10-Q and Annual Reports on Form 10-K, as discussed below. A Form 8-K filing would not be required to be amended to report an update, but registrants would be required to amend a Form 8-K to correct material misstatements or omissions in the Form 8-K disclosure.

Form S-3 Eligibility Not Affected. The Commission acknowledges concerns related to new disclosure requirements that differ from traditional periodic reporting obligations and the potentially disproportionate consequences of loss of short form registration statement eligibility for failure to timely file. As such, the Proposal provides that untimely filing of a Form 8-K relating to an Item 1.05 cybersecurity incident will not result in loss of Form S-3 or other short form eligibility. This is also consistent with how the Commission approaches other Form 8-K items that include subjective materiality determinations.

Safe Harbor from Liability. The Commission also proposes to amend Rules 13a-11(c) and 15d-11(c) under the Securities Exchange Act of 1934, as amended (the "Exchange Act"), to include new Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5. The Commission's view is that the safe harbor is appropriate in this context because the triggering event for proposed Item 1.05 disclosures requires management to make a rapid materiality determination.

Disclosure of Cybersecurity Incidents in Periodic Reports: Updates to Form 8-K Disclosures and Series of Incidents That Are Material in the Aggregate

Updates to Disclosure of Material Incidents. The Proposal would amend Regulation S-K under the Exchange Act to add Item 106(d)(1), which would require registrants to disclose any material changes, additions, or updates regarding cybersecurity incidents previously reported pursuant to proposed Form 8-K Item 1.05, discussed above. Such material changes, additions, or updates would be required to be disclosed in the registrant's corresponding Quarterly Report on Form 10-Q or Annual Report on Form 10-K for the relevant period.

The Proposal provides that updates should include, for example:

— any material effect of the incident on the registrant's operations and financial condition;

— any potential material future impacts on the registrant's operations and financial condition;

— whether the registrant has remediated or is currently remediating the incident; and

— any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.

Incidents That Are Material in the Aggregate. Under the Proposal, disclosure would also be required, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents becomes material in the aggregate. Proposed Item 106(d)(2) of Regulation S-K would require the same content of disclosure required in a Form 8-K for a single material incident—i.e., a description of the incident, data loss, effect on operations, and remediation.

As noted by the Commission, such a disclosure could be triggered by a number of different actions, including where one malicious actor engages in multiple smaller but continuous cyberattacks that in the aggregate have a material impact.

Disclosure of a Registrant's Risk Management, Strategy, and Governance Regarding Cybersecurity Risks

Newly proposed Item 106(b) of Regulation S-K would require detailed disclosure in Annual Reports on Form 10-K regarding a registrant's policies and procedures, if any, for identifying and managing cybersecurity risks.

The Commission notes that the proposed disclosure will be required to provide more consistent and specific information regarding cybersecurity risk management. In pointing to existing risk disclosure practices, the Commission notes that some registrants provide only general, boilerplate disclosure of cybersecurity risk. The Proposal, by contrast, would require a degree of specificity the Commission notes is designed to better inform investors of a company's particular risk profile and how it influences decision-making.

The Commission is seeking detailed disclosure of relevant policies and procedures regarding cybersecurity risk management and strategy, and whether a company has a cybersecurity risk assessment program and undertakes activities to prevent, detect, and minimize the effects of cybersecurity incidents. The new rules would require a registrant to disclose its policies and procedures for identifying and managing cybersecurity risks and threats, including: operational risk; intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk. Further, the rule would require discussion of continuity, contingency, and recovery plans and changes in governance, policies, and procedures stemming from prior cybersecurity incidents.

The proposed rule changes would also require disclosure of a registrant's selection practices and oversight regarding third party service providers. In addition, the rules would require disclosure about the impact of cybersecurity risk on business strategy to enable investors to assess resilience and vulnerability.

Finally, further codifying the 2011 Staff Guidance and 2018 Interpretive Release, registrants would be required to disclose whether cybersecurity-related risks and previous incidents have affected or are reasonably likely to affect a registrant's results of operations or financial condition and whether cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation.

Disclosure of Cybersecurity Governance and Director Expertise

Further drawing from the 2018 Interpretive Release, the Proposal establishes requirements for additional disclosure of board governance and oversight of cybersecurity risks and a description of management's role in assessing and managing such risks. Proposed Item 106(c)(1) of Regulation S-K would require a discussion in a company's Form 10-K regarding: whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks; the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

Registrants would also be required to provide disclosure on management's role in assessing and managing cybersecurity risks and in implementing

cybersecurity policies, procedures, and strategies. Specifically, proposed Item 106(c)(2) of Regulation S-K would require a description of: whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, and the relevant expertise of such persons; whether the registrant has a designated chief information security officer, and if so, to whom that individual reports and their relevant expertise; the processes by which such responsible individuals or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and whether and how frequently such individuals or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

Finally, Item 407 of Regulation S-K would be amended to add Item 407(j), which would require disclosure as to whether any member of the registrant's board of directors has cybersecurity expertise and, if so, the nature of that expertise. The Commission provides several non-exclusive examples of cybersecurity expertise, including whether the director has prior work experience in cybersecurity, has obtained a relevant certification or degree in cybersecurity, or has relevant knowledge, skills, or other background in cybersecurity—including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.

A director with such expertise would not be deemed an expert for any purpose, including under Section 11 of the Securities Act of 1933, as amended (the "Securities Act"), and the Commission clarified that such a director would have no greater duties, obligations, or liability than those of any other director.

Item 407(j) would be applicable for both annual reports and proxy statements. Based on current reporting practices, we would expect many registrants to take advantage of the forward incorporation provision in Instruction G(3) to Form 10-K and include the required 407(j) disclosure only in their definitive proxy statements (filed or required to be filed pursuant to Regulation 14A) or definitive information statement (filed or required to be filed pursuant to Regulation 14C). For registrants that do not utilize forward incorporation or that do not file a proxy statement or information statement (for example, registrants that are wholly owned subsidiaries of other registrants), the disclosure would be required in the Form 10-K.

The Commission is not proposing to add Item 106 or 407(j) disclosure to registration statement Form S-1 or to other Securities Act registration statements.

B. Disclosure by Foreign Private Issuers

Form 20-F

The Proposal would amend Form 20-F to add Item 16J, which would require FPIs to provide the same type of cybersecurity disclosures in their annual reports on Form 20-F as would be required in periodic reports filed by domestic registrants. To this end, proposed Item 16J would list additional requirements for Form 20-F of the same type as included in new Items 106 and 407(j) of Regulation S-K described above. The new Item 16J would not apply to registration statements on Form 20-F.

The Commission did not propose cybersecurity disclosure requirements for Canadian companies filing annual reports on Form 40-F.

Form 6-K

Form 6-K would be amended to add "cybersecurity incidents" as a reporting topic under that Form. The change is intended to provide timely cybersecurity incident disclosure consistent with the general purpose of Form 6-K. That is, FPIs would be required to furnish a Form 6-K to the extent the FPI makes or is required to make a cybersecurity incident public under the laws of its jurisdiction of incorporation, or by filing under the rules of any stock exchange or otherwise distributing such information to its security holders.

C. Inline XBRL

The proposed rules would require registrants to tag information provided in response to Item 1.05 of Form

8-K, Items 106 and 407(j) of Regulation S-K and Item 16J of Form 20-F in Inline XBRL. The tagging would include block text tagging of narrative disclosure, as well as detail tagging of quantitative amounts.

III. General Takeaways

As we noted above, many of the disclosure requirements in the Commission's proposed rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure are a reaffirmation and codification of the 2011 Staff Guidance and the Commission's 2018 Interpretive Release. However, the proposed amendments to Form 8-K—which would require disclosure within four business days after determining that a material cybersecurity incident occurred—and the enhanced requirements for Annual Reports—which would require specific disclosures about, for example, cybersecurity policies and procedures, governance, and oversight—represent significant additions to registrants' disclosure obligations and will require close consideration and careful preparation.

Phase-In

The Proposal does not include timing for effectiveness of any final rules, but we would expect that phase-in of Form 8-K reporting requirements could be quick with requirements for disclosure in annual reports to follow.

Form 8-K: Timing Concerns

A cybersecurity event precipitates a stream of decisions and actions for a company, including technical mitigation work, forensic investigation, regulatory analysis, customer notifications, and interactions with law enforcement, coupled with intense oversight from management and boards of directors. In addition, determining whether a cybersecurity event is material depends on a company having sufficiently reliable information on the nature, scope, and potential impact of the incident, which is often not available immediately following discovery of the incident. Adding time-sensitive reporting requirements to the mix would create additional work streams—and potentially expand the number of individuals involved in sensitive business discussions—at a time when the focus of management and the board is potentially directed elsewhere.

Importantly, the proposed rules provide that the trigger for a required disclosure on Form 8-K is the materiality determination, rather than the initial discovery of a cyber incident, and they also extend safe harbor from liability under Exchange Act Section 10(b) and Rule 10b-5. However, the need for disclosure within four business days of the materiality determination will nonetheless be a significant burden and, in many cases, could require disclosure before facts are fully understood. This may increase the possibility of incorrect or incomplete information being disclosed to the public, and require amending or updating more often than not.

In anticipation of these new rules, companies should review their cybersecurity incident response policies and procedures (as well as disclosure controls and procedures) to ensure they adequately provide for the consideration of materiality for Form 8-K purposes and to assess whether they sufficiently address escalation procedures, governance, and disclosure in light of the Proposal's new requirements. Factors that should be considered in accessing materiality include, among others, the impact of an event on a company's business operations (including disruptions) and financial condition (including losses and costs), data loss, regulatory reporting and impacts, potential litigation, and reputational risk.

No Exceptions Related to Law Enforcement Investigation or Overlapping Reporting Regimes

Interestingly, the Commission's Proposal does not provide for a reporting delay regarding the need to disclose material cybersecurity incidents within four business days in cases where there is an ongoing internal or external investigation related to the cybersecurity incident—including investigations by

law enforcement.[8] The Proposal expressly recognizes that in such cases, a company may be permitted to delay providing public notice about a cyber incident (such as a data breach) under separately applicable state or federal laws in this context. (The reverse could be true as well, where reports may be required under other statutes or regulations even where an incident was determined not to be material to the registrant and no Form 8-K reporting was required.)

However, the Commission maintains that applying such a delay provision in the SEC disclosure context "could undermine the purpose of proposed Item 1.05 of providing timely and consistent disclosure of cybersecurity incidents given that investigations and resolutions of cybersecurity incidents may occur over an extended period of time and may vary widely in timing and scope." As a result, companies would have to meet the new four-business-day disclosure requirement while dealing with other statutory and regulatory obligations and while managing incident response and interaction with law enforcement.[9]

Periodic Reporting: Immaterial Incidents That Are Material in the Aggregate

As discussed above, the Commission's Proposal would require disclosure where a series of previously undisclosed individually immaterial cybersecurity incidents becomes material in the aggregate. The Proposal does not provide guidance on when such a requirement might be triggered beyond the sole example of a malicious actor engaging "in a number of smaller but continuous cyber-attacks related in time and form." While further guidance should be forthcoming in the final rules, registrants should consult with their internal and external cybersecurity advisors to analyze situations where their operations might be materially affected by individually immaterial cyber incidents such that this aggregate disclosure requirement might come into play.

Inline XBRL Tagging

The requirement to provide inline XBRL tagging of all cybersecurity-related information represents a significant increase in the tagging taxonomy. While there may not be significant burden or additional cost associated with tagging in periodic reports, which are already subject to more extensive tagging requirements, additional tagging for Form 8-K could significantly increase the pressure for timely filing. Form 8-K has not previously included inline tagging for narrative information other than the cover page and financial statements. For many companies, this requirement may further increase time pressure to file to allow time for technical tagging.

Policy, Risk, and Oversight Disclosure

The cybersecurity Proposal (and the Commission's March 21, 2022 proposal on climate-related disclosures, which includes very similar provisions related to board oversight disclosure) heralds a new era of rules that specifically address governance issues that the Commission views as requiring granular disclosure about oversight and risk. The proposed rules requiring disclosure about cybersecurity risks, policies, and procedures and about board oversight and management's role in assessing and managing

[8] The Commission noted in the 2018 Interpretive Release that, while an ongoing investigation might affect the specifics in a registrant's disclosure, such an investigation "would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." While the Commission recognizes that a delay in reporting may facilitate a law enforcement investigation, in its view the importance of timely disclosure of cybersecurity incidents justifies not delaying the required SEC reporting.

[9] For example, on March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which imposes federal reporting requirements for cyber incidents and ransomware attack payments. The legislation will require covered critical infrastructure entities to report to the Cybersecurity and Infrastructure Security Agency ("CISA") within 72 hours of forming a reasonable belief that a substantial cyber incident has occurred and within 24 hours of making a ransom payment following a ransomware attack. The reporting requirements will not take effect until implementing regulations are enacted by CISA, which will take time to navigate the rulemaking process. For our full write-up of the Act, see Cleary Gottlieb Alert Memorandum, "*Cyber Incident Reporting for Critical Infrastructure Act* Signed Into Law," Mar. 18, 2022, available here.

cybersecurity risk will require significant and detailed discussion about a company's practices and structure—in addition to the already required disclosure of material risk management and oversight. A significant percentage of companies have started to address oversight of cybersecurity in their annual reports or proxy disclosures, but many will still need to formalize and further define processes and structure. Companies should begin reviewing their current systems and oversight structure and anticipate any desirable changes to board or management structure and procedures.

Board Expertise

Companies will have to consider whether their existing directors qualify as having cybersecurity expertise and what skills or experience will be considered beyond the fairly narrow examples provided by the Commission. Companies may consider updating D&O questionnaires to elicit such information. There may be a relatively small pool of candidates who meet the criteria provided for cybersecurity expertise, though the number of executives and experienced individuals with exposure to cyber-related risk management, oversight, and incident response is increasing by the day. Companies will also have to consider how to create a balanced and effective board in light of numerous other desired qualifications, whether based on regulation or shareholder requests.

…

CLEARY GOTTLIEB