ALERT MEMORANDUM

New SEC Disclosure Rules for Cybersecurity Incidents and Governance and Key Takeaways

August 2, 2023

On July 26, 2023, the U.S. Securities and Exchange Commission (the "SEC" or "Commission") adopted rules to enhance and standardize disclosure requirements related to cybersecurity incident reporting and cybersecurity risk management, strategy, and governance.

The rules were approved by the SEC on a 3-2 vote, with the two Republican commissioners dissenting.[1]

Specifically, the Commission's new cybersecurity disclosure rules:

— 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, and require the disclosure of updates by filing amended Form 8-Ks, to the extent certain information remains unknown at the time of the initial filing;

— 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 and a registrant's cybersecurity governance;

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

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

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

NEW YORK

Francesca L. Odell
+1 212 225 2530
flodell@cgsh.com

Lillian Tsu
+1 212 225 2130
ltsu@cgsh.com

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

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

Synne D. Chapman
+1 212 225 2374
schapman@cgsh.com

[1] The Commission's release, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Release Nos. 33-11216, 34-97989 (the "Adopting Release"), can be found here. The two Republicans commissioners dissented, with Commissioner Peirce arguing the Commission has failed to explain why these rules are necessary in light of prior guidance and Commissioner Uyeda supplementing that the rules "swing a hammer at the current regime and create new disclosure obligations for cybersecurity matters that do not exist for any other topic."

This Alert Memorandum describes the Commission's new cybersecurity disclosure rules and provides some key takeaways.

I. Background of the Rules

The Commission's stated rationale for the new rules is that "under-disclosure regarding cybersecurity persists despite the Commission's prior guidance; investors need more timely and consistent cybersecurity disclosure to make informed investment decisions; and recent legislative and regulatory developments elsewhere in the Federal government, [. . .] while serving related purposes, will not effectuate the level of public cybersecurity disclosure needed by investors in public companies."[2,3]

The rules build 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").[4] 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 companies' 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.[5]

The new rules codify much of the 2011 Staff Guidance and 2018 Interpretive Release, relying upon them as a framework for a more expansive cybersecurity disclosure regime.

II. The New Rules

A. Disclosure by U.S. Registrants

Prompt Disclosure of Material Cybersecurity Incidents on Form 8-K

The new rule amends Form 8-K to add a new Item 1.05, which will require disclosure within four business days after a registrant determines that it has experienced a material cybersecurity incident.[6] Item 1.05 will be required to be filed rather than furnished.

[2] Adopting Release, *supra* note 1, at p. 13.

[3] The Commission conducted 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. *See* Cleary Gottlieb Alert Memorandum, "Cybersecurity: Data Breaches, Ransomware Attacks and Increased Regulatory Focus," Jan. 11, 2022, available here.

[4] *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.

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

[6] The new rules define "cybersecurity incident" as "an unauthorized occurrence, or a series of related unauthorized occurrences, 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" and defines "cybersecurity threat" as "any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." It defines "information systems" as "electronic 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," "cybersecurity threat" and "information systems" are included in Item 106 of Regulation S-K, discussed below and the definition of "cybersecurity incident" applies to new Item 1.05 of Form 8-K.

New Form 8-K Item 1.05 will require registrants to describe:

- the material aspects of the nature, scope, and timing of the incident; and
- the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.

The rule's inclusion of "financial condition and results of operations" is not meant to be exclusive; registrants are expected to consider "qualitative factors alongside quantitative factors in assessing the material impact of an incident."[7] This point remains consistent with the proposed rules and the 2018 Interpretative Release. The Commission has said the "materiality [of a cybersecurity incident] turns on how a reasonable investor would consider the incident's impact on the registrant."[8] Examples of factors that can impact the materiality of a cybersecurity incident include: "harm to a company's reputation, customer or vendor relationships, or competitiveness." The Commission also views "the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal governmental authorities and non-U.S. authorities" as factors to consider when assessing materiality.[9] It is important to note that a registrant's Form 8-K disclosure requirements may be triggered by a material cybersecurity incident impacting systems hosted by a third party.

In a departure from the proposed rule, the new Item 1.05 requirement would not require disclosure regarding an incident's remediation status, whether it is ongoing, or whether data was compromised. However, the Commission notes that some incidents will still necessitate discussion of theft or loss, such as intellectual property loss, business interruption, increased costs of capital, or reputational damage, with the expectation that registrants will make those determinations as part of any materiality analysis.

Further, the Commission is including as Instruction 4 to Item 1.05 that a "registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident."

Timing. The Commission stresses in the Adopting Release that registrants are required to disclose any material cybersecurity incident within four business days after a determination of materiality, acknowledging that "in the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered."[10] Any determination of materiality should be made without unreasonable delay.

Exception for Matters of National Security or Public Safety. The rule adopts a delay provision only in cases where the required disclosure would pose a substantial risk to national security or public safety and the Federal government has certified as such. In new Item 1.05(c), a Form 8-K filing may be delayed up to 30 days "if the Attorney General determines that disclosure [. . .] poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing." An additional delay of 30 days may be allowed if the Attorney General notifies the Commission in writing that disclosure continues to pose a substantial risk to national security. In extraordinary circumstances, a registrant may be able to delay disclosure an additional 60 days (for a total 120-day delay). Any delays beyond the 120-day mark would require relief through Commission exemptive order in addition to the Attorney General's determination.

In connection with this delay provision, the Commission consulted with the Department of Justice to establish an interagency communication process that would allow for any determinations to be conveyed in a timely fashion, and the Department of Justice will notify registrants directly that communication to the Commission has been made.

[7] Adopting Release, *supra* note 1, at p. 29.
[8] Adopting Release, *supra* note 1, at p. 31.
[9] Adopting Release, *supra* note 1, at p. 29.
[10] Adopting Release, *supra* note 1, at p. 32.

Exception for compliance with FCC rule for breaches of CPNI. The Commission acknowledges that the Item 1.05 disclosure requirement contradicts in part the Federal Communications Commission's (the "FCC") notification requirement for breaches of customer proprietary network information ("CPNI"). The FCC's notification rule in the event of breaches of CPNI requires companies to notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") no later than seven business days after reasonable determination of a breach, and instructs companies to refrain from notifying customers or disclosing the breach publicly until seven business days have passed following notification to the USSS and FBI. In order to accommodate registrants subject to this rule, the Adopting Release adds paragraph (d) to Item 1.05, "providing that such registrants may delay making a Form 8-K disclosure up to the seven business day period following notification to the USSS and FBI specified in the FCC rule, with written notification to the Commission."[11]

Form S-3 Eligibility Not Affected. The rule 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, consistent with how the Commission approaches other Form 8-K items that include subjective materiality determinations.

Safe Harbor from Liability. The Adopting Release also amends 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 Item 1.05 disclosures requires management to make a rapid materiality determination.[12]

Updating vs. Amending. In a departure from the proposed rule, the Adopting Release no longer permits updates regarding cybersecurity incidents in a registrant's periodic annual or quarterly reports. To the extent information required to be disclosed pursuant to new Item 1.05(a) at the time of the original 8-K filing is not yet determined or is unavailable, registrants will now be required to file an amendment to the original Form 8-K disclosing such information within four business days after the registrant determines such information or after such information becomes available. As with the original filing, any determination of materiality should be made without unreasonable delay. Registrants would still be required to amend a Form 8-K to correct material misstatements or omissions at the time the original Form 8-K disclosure was made as well.

Aggregation. The Commission is also no longer adopting proposed Item 106(d)(2) of Regulation S-K, regarding disclosure in periodic reports of aggregated incidents, in response to concerns that the proposed aggregation requirement was too difficult to apply. However, the definition of "cybersecurity incident" used in Item 106 of Regulation S-K and Item 1.05 of Form 8-K has been expanded to cover "a series of related unauthorized occurrences." The Commission is still focused on ensuring that cyberattacks that may compound over time, rather than present as a discrete event, are still considered for a registrant's disclosure. The Commission stated in the Adopting Release that if a registrant "finds that it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each by itself immaterial."[13] The Adopting Release then goes on to provide the following examples:

- the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material; or

[11] Adopting Release, *supra* note 1, at p. 42.
[12] Adopting Release, *supra* note 1, at p. 40.
[13] Adopting Release, *supra* note 1, at p. 53.

- a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially.

Aggregated incidents would be required to be reported when a registrant determines that together they constitute a material cybersecurity incident.

Timing for Compliance. Item 1.05 disclosure will be required beginning December 18, 2023.

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

New Item 106(b) of Regulation S-K requires detailed disclosure in Annual Reports on Form 10-K regarding a "registrant's processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes."

The streamlined rule requires a degree of specificity that the Commission notes is designed to allow investors to ascertain a registrant's cybersecurity practices, such as whether they have a risk assessment program in place, with sufficient detail for investors to understand the registrant's cybersecurity risk profile.

The new rule requires a registrant to address:

- whether and how the described cybersecurity processes in Item 106(b) have been integrated into the registrant's overall risk management system or processes;
- whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
- whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

The Commission stresses that registrants should additionally disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes.

In an effort to further codify the 2011 Staff Guidance and 2018 Interpretive Release, registrants are also required to disclose whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how. Registrants will also need to disclose how they engage assessors, consultants, auditors, or other third parties in connection with their cybersecurity, though disclosing the names of those third parties is not required.

Item 106 disclosure will not be added as a separate form requirement to registration statement Form S-1 or to other Securities Act registration statements.

Disclosure of Cybersecurity Governance

Further drawing from the 2018 Interpretive Release, the rule 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. Item 106(c)(1) of Regulation S-K requires registrants to describe the board's oversight of risks from cybersecurity threats, and, if applicable, identify any board committee or subcommittee responsible for such oversight, as well as describe the processes by which the board or such committee is informed about such risks. The Commission declined to include Item 407(j) of Regulation S-K in the final rules, which would have required registrants to disclose the cybersecurity expertise of a board's directors.

Registrants are also required to provide disclosure on management's role in assessing and managing a registrant's material risks from cybersecurity threats. Item 106(c)(2) of Regulation S-K asks registrants to address:

- whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such

detail as necessary to fully describe the nature of the expertise;

- the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

The Commission stresses the list in 106(c)(2) is meant to be non-exhaustive.

Timing for Compliance. Item 106 disclosure will be required beginning with annual reports for fiscal years ending on or after December 15, 2023.

B. Disclosure by Foreign Private Issuers

Form 20-F

The Adopting Release amends Form 20-F to add Item 16K, which requires FPIs to provide the same type of cybersecurity disclosure on risk and governance in their annual reports on Form 20-F as would be required in annual reports filed by domestic registrants. New Item 16K lists requirements for Form 20-F of the same type as included in new Item 106 of Regulation S-K described above. Item 16K disclosure will be required beginning with annual reports for fiscal years ending on or after December 15, 2023. The new Item 16K does not apply to registration statements on Form 20-F.

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

Form 6-K

Form 6-K is being 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 are 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. Unlike domestic registrants, FPIs will not need to comply with the four business-day disclosure requirement under Form 8-K, but rather will need to comply with any applicable home country requirements, consistent with their other Form 6-Ks.

Similar to the Form 8-K changes, the Form 6-K disclosure will be required beginning December 18, 2023.

C. Inline XBRL

The rule requires registrants to tag information provided in response to Item 1.05 of Form 8-K, Item 106 of Regulation S-K and Item 16K of Form 20-F in Inline XBRL. The tagging includes block text tagging of narrative disclosure, as well as detail tagging of quantitative amounts. The structured data requirements will have a staggered compliance date of one year.

III. General Takeaways

Disclosure Timing Concerns

Upon discovery of a potential cyber incident, domestic registrants will be under pressure to make a materiality decision, and once an incident has been determined to be material, will need to file a Form 8-K within four business days. The prospect of the SEC and investors scrutinizing a materiality decision may incentivize companies to make a disclosure before they have complete information. It can often take weeks to determine the full scope of an incident, including whether a threat actor has exfiltrated data and, if so, what data. If a registrant does not disclose an incident within the four business-day window after discovery, it will be important to memorialize the lack of a materiality determination or the lack of available information to make such a decision. When a registrant does disclose a cyber incident, it will want to either disclose the date of the materiality determination, to be able to confirm it was within four business days of making the filing, or state that the company is still evaluating materiality if the disclosure is made after the initial four business days. In the latter case, a

company would then need to amend its original Form 8-K once a materiality decision has been made.

Updating and Amending

Alongside a concern for timely reporting is a concern for accurate reporting. The Commission made a point of reminding registrants in the Adopting Release that they "may have a duty to correct prior disclosure that the registrant determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made (for example, if the registrant subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made (for examples, when the original statement is still being relied on by reasonable investors). Registrants should consider whether they need to revisit or refresh previously disclosure, including during the process of investigating a cybersecurity incident."[14]

Unfortunately, the requirement to disclose as soon as a determination of materiality is made means registrants will likely be updating and correcting Form 8-Ks more frequently than was previously the case, given the potential uncertainty of the information within the allotted time period for initial disclosure.

Preparedness Concerns

An aggressive reporting regime emphasizes the need for registrants to have an incident response plan and forensic and other experts on retainer in the event of an attack, in order to attempt to quickly determine the information needed to make a disclosure decision.

Compounding these concerns is the relatively fast phase-in timing, with compliance with the new Form 8-K and Form 6-K disclosure required beginning December 18, 2023. Registrants that have been waiting to refine their incident response plans to accommodate the final rules will be under time pressure to prepare for the end of this year.

No Forward Incorporation into Proxy Statement Disclosure

The disclosure required under new Item 106 of Regulation S-K will be required to be included in a registrant's Annual Report on Form 10-K. Given that the requirement is included in Part I of Form 10-K, registrants will not be able to avail themselves of the forward-incorporation into a registrant's proxy statement, allowed by Instruction G(3) for items included in Part III of Form 10-K.

Exceptions Not Available to FPIs

As currently constructed, the Commission's exception for cybersecurity incidents that may be a matter of national security or public safety does not appear to be available to FPIs, nor does the FCC exception. The exceptions are built into Items 1.05(c) and (d) of Form 8-K, respectively. Barring additional guidance from the Commission, an FPI will be required to disclose what it (i) makes or is required to make public pursuant to the law of the jurisdiction of its domicile or in which it is incorporated or organized, (ii) files or is required to file with a stock exchange on which its securities are traded and which was made public by that exchange, or (iii) distributes or is required to distribute to its security holders, consistent with the general disclosure requirements under Form 6-K.

No Board Expertise Disclosure Requirement

In a pleasant turn of events, the Commission chose to drop its proposal to add Item 407(j) of Regulation S-K, which would have required registrants to disclose the cybersecurity expertise of a board's directors. As a result of comments received, the Commission was convinced that "effective cybersecurity processes are designed and administered largely at the management level, and that directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise, as they do with other sophisticated technical matters."[15]

[14] Adopting Release, *supra* note 1, at p. 51.

[15] Adopting Release, *supra* note 1, at p. 85.

Board and Management Structure

The removal of the board expertise disclosure requirement and paring back of some of the governance disclosure requirements was noted by Commissioner Peirce as an improvement from the proposal.[16] Registrants that have not already made changes in the wake of the proposal may want to review their board and management structure and policies to prepare for discussion of the same in the their Form 10-K or Form 20-F. Annual comparison and benchmarking exercises and adoption of emerging best practices as described in disclosure will likely be added to the overall governance review process and companies should be prepared for the disclosure rules to ultimately lead to changes in their corporate policy and practice.[17]

Commission Overreach?

Commissioners Peirce and Uyeda both expressed concern regarding the need for the new rules and the Commission's mandate, with Commissioner Peirce saying the rule "reads like a test run for future overly prescriptive, overly costly disclosure rules covering a never-ending list of hot topics." There remains a risk, as the Commission continues to require prescriptive disclosure in areas of non-financial risk, that the Commission could, through comments on disclosure or enforcement actions, further change how governance is undertaken by public companies.

…

CLEARY GOTTLIEB

[16] Commissioner Peirce noted in her statement "Nevertheless, even these pared back disclosures may serve to drive companies to spend resources on compliance with our rules and conformity with other companies' disclosed practices, instead of on combatting cyber threats as they see fit. Once the SEC can peer into how all public companies handle cybersecurity, the temptation to micromanage their operations will only grow."

[17] For an additional discussion of the Commission's disclosure agenda, *see* Cleary Gottlieb Alert Memorandum, "Turning a Corner on Corporate Governance: The SEC's Disclosure Agenda," Jan. 17, 2023, available here.

Summary of New Requirements[18]

Item	Summary Description of the Disclosure Requirement
Regulation S-K Item 106(b) – *Risk management and strategy*	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
Regulation S-K Item 106(c) – *Governance*	Registrants must: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 8-K Item 1.05 – *Material Cybersecurity Incidents*	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: - Nature, scope, and timing; and - Impact or reasonably likely impact. An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety. Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.
Form 20-F	FPIs must: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing material risks from cybersecurity threats.

[18] Adopting Release, *supra* note 1, at p. 12.

Form 6-K	FPIs must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders.