WILMERHALE

Preparing for New Cybersecurity Disclosures

AUGUST 11, 2023

Public companies will soon be required to provide increased transparency about cybersecurity incidents, risk management, strategy and governance as a result of new rules adopted by the Securities and Exchange Commission (the "SEC" or "Commission") on July 26, 2023.[1] These new disclosure requirements represent a significant expansion of the existing SEC disclosure guidance, which dates back to 2011 and 2018, and represent the SEC's first disclosure requirements explicitly referring to cybersecurity risk and incident reporting in current and periodic reports.

Following an overview of the new rules, we identify below practical considerations for registrants in preparing for the new disclosure requirements.

Background

Previously, cybersecurity risk and incident disclosures in SEC reports were informed primarily by SEC staff guidance published in 2011 and Commission level guidance published in 2018 (the "2011 Staff Guidance" and "2018 Interpretive Guidance," respectively). In the 2011 Staff Guidance, the SEC Division of Corporation Finance staff acknowledged that although there were no disclosure rules explicitly referring to cybersecurity risks and incidents, registrants may be obligated to disclose such risks and incidents, as well as material information regarding such risks and incidents, when making other required disclosures pursuant to obligations under existing rules, such as Regulation S-K Items 101 (description of business), 103 (legal proceedings), 105 (risk factors), 303 (management's discussion and analysis of financial condition and results of operation), and 307 (disclosure controls and procedures), as well as certain provisions in the Accounting Standards Codification.[2] The 2018 Interpretive Guidance added to the SEC staff's prior

[1] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,* Release No. 33-11216, 88 Fed. Reg. 51896 (adopted July 26, 2023), https://www.sec.gov/files/rules/final/2023/33-11216.pdf [hereinafter Adopting Release].

[2] *See* CF Disclosure Guidance: Topic No. 2—Cybersecurity (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

guidance on cybersecurity disclosures by discussing potential reporting obligations under Regulation S-K Item 407 (corporate governance), Regulation S-X and Regulation FD, noting that registrants may provide current reports to maintain the accuracy and completeness of effective shelf registration statements and encouraging companies to consider whether insider trading restrictions should be put into effect following a cybersecurity incident and before disclosure surrounding such incident is made.[3]

On March 9, 2022, the SEC proposed new rules to increase and standardize cybersecurity disclosures by public companies subject to reporting requirements under the Securities Exchange Act of 1934, as amended (the "Exchange Act").[4] The SEC reopened the comment period on the proposal twice and received over 150 comment letters. Commenters raised various concerns about the rule proposals, with a significant number of comments concerning the timing of the proposed incident disclosure requirement in particular, as well as the proposed board expertise disclosure requirement.[5]

On July 26, 2023, in a 3-2 vote, the SEC adopted new rules for public companies that require current reporting of material cybersecurity incidents, as well as annual disclosures about cybersecurity risk management, strategy, and governance. The new rules and amendments affect Forms 8-K, 6-K, 10-K and 20-F, and include inline XBRL tagging requirements.[6] The new requirements apply broadly to all public companies, including foreign private issuers, emerging growth companies and smaller reporting companies.

The new rules will significantly affect the way public companies disclose cyber incidents and matters relating to their cybersecurity oversight. In adopting the new requirements, the SEC confirmed that the 2018 Interpretive Release and 2011 Staff Guidance remain applicable and should be used to inform potential disclosure obligations relating to cyber incidents that are not specifically addressed in the latest rule requirements.[7]

The implementation dates under the new rules, which are outlined in the table below, are extremely tight. In general, companies other than smaller reporting companies will be required to comply with the new current reporting requirements in Forms 8-K and 6-K beginning December 18, 2023. Smaller reporting companies will be subject to the new current reporting requirements on June 15, 2024. For all companies, the annual reporting requirements in Forms 10-K and 20-F will apply starting with their Forms 10-K and 20-F filed in early 2024.

---

[3] *See Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release No. 33-10459, 83 Fed. Reg. 8166 (published Feb. 21, 2018).
[4] *See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release No. 33-11038, 87 Fed. Reg. 16590 (proposed Mar. 9, 2022), https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf.
[5] Adopting Release at 10.
[6] *Id.* at 11-13.
[7] *Id.* at 95-96.

Summary of New Disclosure Requirements in Current Reports

The new rules establish a real-time reporting requirement for material cybersecurity incidents, which generally applies separately and in parallel with any other cyber reporting obligations the registrant is subject to under federal, state or foreign law.

What must be included in a Form 8-K?

Pursuant to Item 1.05 of Form 8-K, upon experiencing a material cybersecurity incident, a registrant must disclose (i) the nature, scope and timing of the incident and (ii) the material or reasonably likely material impact on the registrant, its financial condition and its results of operation.

Amendments to Form 8-K. Under new Item 1.05 of Form 8-K, a registrant that experiences a material cybersecurity incident must report 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."

In response to public comment about the scope of the new rule, the SEC indicated that it adopted this language in an attempt to better focus the disclosure on the effects of a material cybersecurity incident, rather than specific details regarding the incident itself. Notably, in a departure from the proposal, the final rule does not require companies to discuss the cybersecurity incident's remediation status, if it is ongoing, or whether data were compromised. Nor does the rule require disclosure of the specific or technical information about the registrant's planned response or its cybersecurity systems, networks and devices, or potential system vulnerabilities to such a degree of detail as would impede the registrant's response or remediation of the incident.

Cybersecurity Incident. For disclosure purposes, a "cybersecurity incident" is defined 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." The "series of related unauthorized occurrences" language reflects the SEC's stated view that "cybersecurity incident" should be viewed broadly. This language is a change from the proposal, which would have required disclosure in periodic reports when it became known to management that a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate.[8] The adopting release includes examples of situations that may trigger Item 1.05 disclosure, including incidents occurring on third-party systems or accidental exposures of customer data that results in unauthorized access to that data.[9] This same definition of cybersecurity incident and broad interpretation applies to Item 1.05 of Form 8-K as it does for purposes of the disclosures provided pursuant to Regulation S-K Item 106 (discussed below).

[8] *Id*. at 47, 52.
[9] *Id*. at 78-79.

Third-Party Service Providers. Registrants are not exempt from providing disclosures regarding cybersecurity incidents on third-party systems they use, nor will they receive a safe harbor for information disclosed about third-party systems they use. Depending on the circumstances of a cybersecurity incident that occurs on a third-party system, disclosures may be required by either or both of the service provider and customer. Because the definition of "information systems" covers electronic information resources "owned or used by the registrant," a registrant is required to disclose a cybersecurity incident suffered by a third-party information technology service provider's system in a current report on Form 8-K if such incident has a material impact on the registrant. The SEC noted in the adopting release that registrants need only disclose information made available to them, and are generally not required to conduct additional inquiries beyond their regular communications with third-party service providers pursuant to those contacts and in accordance with such registrant's disclosure controls and procedures.[10] With this in mind, we recommend that registrants carefully review their policies and procedures with respect to oversight of third-party systems.

Materiality. Disclosure is required under Item 1.05 of Form 8-K only if the registrant determines that the cybersecurity incident it experienced is "material." Whether a cybersecurity incident is "material" is to be analyzed under the traditional securities law definition of materiality, meaning an incident is material if "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." Registrants must consider both qualitative and quantitative factors when assessing the materiality of a cybersecurity incident.[11]

Timing of Disclosure and Permitted Delays. An Item 1.05 Form 8-K must be filed within four business days of a registrant determining it has experienced a material cybersecurity incident. Per Instruction 1 to Item 1.05, a registrant's materiality determination must be made without unreasonable delay after discovery of the incident. This timing standard is a change from the proposal, which would have required the materiality determination to be made "as soon as reasonably practicable after discovery of the incident." The adopting release includes examples of what would constitute "unreasonable delay," including when intentionally delaying a board or committee meeting on the materiality determination past the normal time it takes to convene its members, or revising policies and procedures to delay a determination by extending the registrant's incident severity assessment deadlines.

At the Open Meeting of the SEC held July 26, 2023, Chair Gensler emphasized that the four-business day period to file an Item 1.05 Form 8-K begins when a registrant determines a cybersecurity incident is material, rather than when the registrant discovers that the cybersecurity incident occurred and/or is ongoing.[12]

---

[10] *Id.* at 31.
[11] *See id.* at 37-39 for a discussion of factors that may be relevant to the materiality analysis and the timing of that determination.
[12] U.S. Securities and Exchange Commission, *2023 07 06 Open Meeting*, https://www.youtube.com/watch?v=pWpel8PEy1Y.

In response to public comments raising concerns with the four-business day deadline, the SEC added paragraph (c) to Item 1.05, which allows for delayed Form 8-K reporting in extremely limited circumstances. Registrants may delay filing an Item 1.05 Form 8-K where the United States Attorney General determines that disclosure under Item 1.05 poses a substantial risk to national security or public safety, and the Attorney General notifies the SEC of such determination in writing. Under these circumstances, the registrant may delay providing an Item 1.05 Form 8-K filing for the time period specified by the United States Attorney General, which may be up to 30 days from the date when the disclosure under Item 1.05 was otherwise required, subject to an additional extension period of up to another 30 days. In extraordinary circumstances involving national security (but not public safety), a further extension for an additional period of up to 60 days may be available. If the Attorney General indicates that further delay is necessary, the SEC will consider such request and may grant such relief through Commission exemptive order.

A registrant will be notified by the Department of Justice whenever the Attorney General communicates a determination to the SEC so that such registrant may delay filing its Form 8-K. Based on written statements from the Federal Bureau of Investigation (the "FBI"), additional guidance from that agency and the Department of Justice concerning the intake and evaluation process for requests to delaying filing for reasons of national security or public safety is anticipated in the weeks and months ahead.

In response to public comments regarding conflicts with other Federal laws and regulations, the SEC added paragraph (d) to Form 8-K Item 1.05, which also allows delayed 8-K reporting in certain circumstances. Specifically, registrants may delay filing an Item 1.05 Form 8-K where the data breach involves customer proprietary network information ("CPNI") that must be disclosed pursuant to certain rules of the Federal Communications Commission (the "FCC"). Registrants covered by 47 C.F.R. § 64.2011 are required to notify the United States Secret Service (the "USSS") and the FBI no later than seven business days after reasonable determination of a CPNI breach and to refrain from notifying customers or disclosing the breach publicly until seven business days after the USSS and FBI were notified. Because of this, paragraph (d) allows registrants to delay making an Item 1.05 Form 8-K report up to seven days after the USSS and FBI are notified of a data breach involving CPNI covered by the applicable FCC regulations, provided that written notification is given to the SEC by the date disclosure required by Item 1.05 was otherwise required to be made.

The new rules require foreign private issuers to furnish on Form 6-K information about material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders. This reporting requirement is consistent with other items that foreign private issuers are required to report on Form 6-K. Unlike reports under Item 1.05 of Form 8-K, Form 6-K does not include a four-business day reporting deadline.

Amending Prior Item 1.05 Form 8-K Disclosures. The SEC acknowledged in its adopting release that certain information responsive to the requirements of new Item 1.05 may not be determined or

might be unavailable at the time the Item 1.05 Form 8-K is required to be filed.[13] In response to public comments, the SEC revised Instruction 2 to Item 1.05, which now provides that whenever a registrant determines information required to be disclosed under Item 1.05 is not available or determined at the time of the required filing, then the registrant must (i) include a statement to this effect in its Item 1.05 Form 8-K and (ii) within four business days after the registrant, without unreasonable delay, determines such information or such information becomes available, file an amendment to the initial Item 1.05 Form 8-K. This is a change from the proposed rule, which would have required updated incident disclosure in companies' periodic reports.[14]

Amendments to the Eligibility of Provisions of Form S-3 and Form SF-3 and Safe Harbor Provisions in Exchange Act Rules 13a-11 and 15d-11. Similar to other Form 8-K items that rely on materiality determinations, a registrant's untimely filing of an Item 1.05 Form 8-K will not result in a loss of Form S-3 or SF-3 eligibility. Further, Rules 13a-11 and 15d-1 have been amended to include new Item 1.05 of Form 8-K in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) of and Rule 10b-5 under the Exchange Act.

Summary of New Disclosure Requirements in Periodic Reports

The rule amendments add new Item 106 to Regulation S-K, which requires enhanced and standardized disclosure of registrants' cybersecurity risk management, strategy, and governance. New Item 106 disclosures will be required to be reported in annual reports on Form 10-K, whether or not similar information will be included in a registrant's proxy statement in the discussion of cybersecurity oversight or otherwise. Similar disclosure requirements were added to Form 20-F as new Item 16K. The new requirements include:

Amendments to Forms 10-K. New Item 1C to Form 10-K directs registrants to provide the information required by new Item 106 of Regulation S-K. At a high level, registrants must disclose:

- Company processes, if any, to assess, identify, and manage material cyber security risks;
- Management's role and expertise in assessing and managing material cybersecurity risks; and
- Board of directors' oversight of cybersecurity risks.

Risk Management and Strategy. Pursuant to new Item 106(b) of Regulation S-K, a company must disclose their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats. Such disclosures must be provided in sufficient detail for a reasonable

[13] Adopting Release, *supra note* 1, at 50-51.
[14] *Id*. at 47.

investor to understand such processes. New Item 106(b)(1) includes the following non-exhaustive list of disclosure items a registrant should address:

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

In addition to the items above, the SEC stated in its adopting release that "registrants should additionally disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes."[15] Notably, in response to some commenters, the SEC clarified in the adopting release that disclosure about third-party service providers need not name the specific third parties nor describe the services that they provide.[16]

The final rules also add new Item 106(b)(2) of Regulation S-K, which requires a registrant to disclose in its annual report a description of "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."[17]

Governance. Pursuant to new Item 106(c) of Regulation S-K, a registrant will be required to disclose the board's oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats. In a departure from the proposed rule, disclosure as to a registrant's board of directors' cybersecurity expertise is not required.[18]

Specifically, Item 106(c)(1) of Regulation S-K will require a description of a registrant's board of directors' oversight of risks posed by cybersecurity threats and, if applicable, identification of any committee or subcommittee of the board responsible for cybersecurity risk oversight and a description of the processes by which the board or applicable committee is informed about risks from cybersecurity threats. The SEC noted in its adopting release that, despite comments to the contrary, Item 106(c)(1) serves a distinct purpose from the existing Item 407(h) requirement that a company disclose its board's leadership structure and administration of risk oversight *generally*.[19]

---

[15] *Id.* at 63.
[16] *Id.* at 64.
[17] *Id.* at 63.
[18] *Id.* at 83-85.
[19] *Id.* at 69.

Item 106(c)(2) of Regulation S-K will require a registrant to disclose annually management's role in managing and assessing the registrant's material risks from cybersecurity threats. The rule provides the following non-exclusive list of disclosure items a registrant should address in disclosing such role by their management:

- Whether and which management positions or committees are responsible for assessing and managing risks from cybersecurity threats, and the relevant expertise of such persons;
- The processes by which such persons or committees become informed of 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 any committee or subcommittee).

The discussion of the relevant experience of persons responsible for assessing and managing cybersecurity risk must be in such detail as "necessary to fully describe the nature of the expertise." Instruction 2 to Item 106(c) states that such discussion may include prior cybersecurity work experience, any relevant degrees or certifications, or any knowledge, skills or additional background in cybersecurity.

Definitions. New Item 106(a) of Regulation S-K contains definitions for the following terms as they appear in that section: "cybersecurity incident," "cybersecurity threat," and "information systems." As discussed above, the definition of "cybersecurity incident" was revised from the proposal to include the phrase "series of related unauthorized occurrences," to reflect the SEC's view that "a series of related occurrences may collectively have a material impact or reasonably likely material impact and therefore trigger Form 8-K Item 1.05, even if each individual occurrence on its own would not rise to the level of materiality."[20] The definition of "cybersecurity threat" was revised to conform to the cybersecurity incident definition in clarifying that unauthorized occurrences are those "on or conducted through a registrant's information systems." Regarding the definition of "information systems," the SEC inserted "electronic" before "information resources" in the final definition of information systems in response to public comments and to clarify that the definition does not cover hard-copy resources.[21] The SEC declined to define any other terms, including "cybersecurity."[22]

Timing

The above changes become effective September 5, 2023. As noted above, the timing to implement these new disclosure requirements is extremely tight. The following chart summarizes

[20] *Id.* at 76.
[21] *Id.*
[22] *Id*. at 80-81.

the compliance dates, including applicable transition delays that apply to smaller reporting companies:[23]

	Company That Is Not a Smaller Reporting Company	**Smaller Reporting Company**
Incident reporting on Item 1.05 of **Form 8-K (and Form 6-K** if otherwise disclosed in a foreign jurisdiction, to any stock exchange, or to security holders**)**	Beginning on December 18, 2023	Beginning on June 15, 2024
Inline XBRL tagging of Item 1.05 incident reporting on **Form 8-K (and Form 6-K)**	Beginning on December 18, 2024	
S-K 106 disclosure on **Form 10-K (and Form 20-F Item 16K)**	Beginning with annual reports for fiscal years ending on or after December 15, 2023 *For calendar year-end companies this means the Form 10-K filed in 2024 with respect to the year ending December 31, 2023*	
Inline XBRL tagging of S-K 106 disclosure **on Form 10-K (and Form 20-F Item 16K)**	Beginning with annual reports for fiscal years ending on or after December 15, 2024 *For calendar year-end companies this means the Form 10-K filed in 2025 with respect to the year ending December 31, 2024*	

[23] *Id.* at 107.

Structured Data Requirements

Consistent with other recent SEC rulemaking, the new disclosures must also be tagged using inline XBRL, including by detail tagging quantitative amounts and block text tagging narrative disclosures. The compliance date, however, for tagging requirements is later than the date by when the new disclosure rules apply, as reflected in the table above.

Practical Considerations

For registrants that experience a cyber event, the immediate impact of these new rules will be significant. The rules require focused disclosure controls and procedures, and satisfying the new current reporting obligation hinges on effective communications among many potential stakeholders, including technology teams, external reporting groups, legal teams, management, consultants, and auditors. While many registrants already have in place disclosure controls and procedures relating to cyber events, the new requirements should require, at a minimum, giving those controls and procedures a fresh look. Registrants should also start the education process with the appropriate stakeholders now so that they are able to coordinate efficiently once these new rules take effect. We provide some suggestions below to assist in these preparations.

What To Consider When Assessing Materiality. As noted above, registrants must consider both qualitative and quantitative factors when assessing whether the impact of a cybersecurity incident is material. Informed in part by commentary in the adopting release and by our experience helping company's evaluate disclosure obligations under the 2011 Staff Guidance and 2018 Interpretive Guidance, below are some of the factors we believe registrants may generally want to keep in mind when evaluating materiality.

Quantitative Considerations

- Reasonably expected percentage impact on revenue due to lost sales of products or services;
- Reasonably expected percentage impact on net income due to lost revenues, expenses associated with containing and remediating the incident (including, as applicable, any ransom payment) and other expected expenses (including responding to regulatory and legal proceedings and any voluntary actions to mitigate harm to affected individuals); and
- Reasonably expected percentage impact on total and current assets of expenses associated with the incident.

Qualitative Considerations

- Relative importance of the systems affected by the incident to the registrant's operations (including how long those systems may be inoperable);
- Duration of the incident, method of incident detection and readiness of the response to halt the incident;
- Ability to restore affected systems and the expected integrity of those systems once restored;
- Nature and scope/magnitude of the information that has been improperly accessed or exfiltrated;
- Effect of the incident on key systems or information that the registrant considers its "crown jewels";
- Harm to the registrant's reputation and brand perception;
- Impact on the registrant's supply chain and operations, including likelihood of consequential harms resulting from delays or other effects of the incident;
- Impact on relationships with customers (both near-term and over time);
- Impact on relationships with suppliers and other business partners (both near-term and over time);
- Effect on the registrant's competitive position relative to its peers (both near-term and over time);
- Likelihood of regulatory actions by various governmental authorities; and
- Likelihood of private litigation from individuals whose information has been compromised.

Considerations That Typically Will Not Affect the Materiality Analysis

- Whether the affected system was owned or operated by the registrant or a third-party;
- Inability to determine the full extent of the incident;
- Ongoing nature of the registrant's internal investigation; and
- Timing of sharing information about the incident with governmental authorities or others.

Controls and Procedures. First and foremost, we recommend that registrants implement cybersecurity disclosure controls and procedures, if they are not already in place. To the extent that registrants have gaps in their existing cybersecurity disclosure controls and procedures, we recommend that they take the time now to review and enhance their overall cybersecurity risk management strategy and governance process. This is a particularly crucial step given the SEC's focus in recent enforcement actions on controls and procedures, as well as the new Regulation S-K Item 106 disclosure requirements.

Incident Response Plans and Procedures. Having an Incident Response Plan ("IRP") is one common element of a mature cybersecurity program. As registrants prepare for the new SEC disclosure rules, we recommend that they review and update their processes for responding to

cybersecurity events. As part of this review, registrants with an existing IRP and any associated playbooks and procedures should make sure that these materials are updated to ensure that the materiality determination for a cybersecurity incident is not "unreasonably delayed" and give consideration to any definitional differences between material cyber incidents for SEC disclosure purposes and cyber incidents described within the IRP that may be subject to other reporting regimes. Registrants without an existing IRP are well-advised to prepare one.

A comprehensive IRP would include, among other things:

- The goals and scope of the plan;
- A process for identifying, categorizing, escalating, investigating, and remediating potential incidents;
- Defined roles and responsibilities for the incident response team (including clear levels of decision-making authority);
- A process for external and internal communications and information sharing;
- A process for SEC disclosure regarding cybersecurity events; and
- A process to review and revise the IRP (as necessary) post-incident to account for lessons learned.

We recommend that in reviewing IRPs, registrants pay particular attention to the communications pathway to ensure that the appropriate decision-makers are timely alerted to evaluate materiality as required by the new SEC disclosure rules and to consider the need to close the trading window and that there are procedures in place to document both the basis of the materiality analysis as well as the reasonableness of the time it took to make that determination.

Furthermore, IRPs should include a process to evaluate whether it is necessary to request a national security/public safety exception and a process to proceed with the materiality assessment should the request to delay disclosure be denied. We expect that the exception will apply in only very limited circumstances, so registrants should discount the likelihood of its availability. Registrants should also ensure that there are processes in place to address potential inconsistencies in communications over time as the investigation continues to unfold and more information is gleaned after the initial disclosure. Additionally, as time is of the essence with respect to incident detection, response, and disclosure, registrants may find it helpful to create a communications playbook with pre-approved language for public-facing statements to ensure consistency in communications. Finally, after reviewing an IRP, we recommend that registrants test their revised IRP using a scenario that would require disclosure under the SEC's new rule.

Reviewing Allocation of Oversight Responsibilities & Voluntary Disclosures. Many registrants have their board (or a committee of their board) oversee management's control of cybersecurity risks as part of their overall risk oversight responsibilities. Some registrants also currently have a separate committee of their board dedicated specifically, in whole or in part, to oversight of cybersecurity matters. Further, many registrants already voluntarily disclose their board's oversight of

management's cybersecurity risk practices in their proxy statements, generally as part of the discussion of board committees (and their responsibilities) and/or their board's risk oversight functions. With new Regulation S-K Item 106 now requiring companies to make certain disclosures in Form 10-Ks about management's role and expertise in assessing and managing cybersecurity related risks, as well as the board's role in overseeing management's control of cybersecurity risk, we recommend that registrants review their current allocation of cybersecurity risk management and oversight and consider whether any changes should be made. Further, we recommend that registrants that have previously provided disclosures in their proxy statements or elsewhere about their cybersecurity risk management practices ensure that such disclosures both adequately reflect their current allocation of cybersecurity risk management and oversight responsibilities between management and the board and are consistent with new cybersecurity risk disclosures to be made in their Form 10-K pursuant to new Regulation S-K Item 106. Additionally, we recommend that registrants confirm that their disclosures do not conflict with any other requirements relating to governance and board reporting to which they may be subject (e.g., NYDFS Part 500).

Additional Disclosure Considerations. Disclosures must be carefully drafted and should be the product of careful coordination with the appropriate legal and corporate teams as well as the appropriate security and technical personnel. We recommend that registrants, in addition to evaluating their IRPs, consider whether other privacy and cybersecurity-related rules are applicable and pay close attention to the extent to which compliance obligations with other rules or requirements impact the framing of disclosures. Registrants should expect greater scrutiny of their public filings with respect to cybersecurity moving forward and the information provided may contribute to possible regulatory enforcement or litigation. Additionally, to the extent that registrants have previously made disclosures related to cybersecurity in their public findings, these companies should consider reviewing their prior risk factor and proxy statement disclosures and assessing the extent to which these need to be enhanced or revised moving forward. Finally, registrants should confirm that the disclosures are, in fact, accurate. For example, to the extent that a registrant makes a representation that a committee of the board meets quarterly to evaluate cybersecurity risk, registrants should expect those quarterly reports to be requested by regulators in connection with investigations of cybersecurity incidents.

For some registrants, there may be additional rules and regulations related to cybersecurity compliance and oversight depending on the nature of the registrant's business, the industry/sector in which they operate, and the types of data that they may hold or access. These additional requirements should be prominent considerations as such registrants draft cyber-related disclosures for purposes of the new SEC disclosure rules.

Select Departures from the Proposing Release

The final rule retreated from a few of the amendments initially proposed. Some of these changes are noted throughout this client alert. For ease of reference, we have listed below noteworthy changes from the proposal:

- Revised Instruction 2 to Item 1.05 of Form 8-K and omitted a proposed Regulation S-K Item 106 amendment, such that certain updated incident disclosures (i.e., information that was not known at the time of the initial filing) are to be reported on an amended Form 8-K instead of provided on an ongoing basis in Forms 10-Q and 10-K.[24]
- Added Instruction 4 to Item 1.05 of Form 8-K, which clarifies 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 registrant's response or remediation of the incident."[25]
- Removed a proposed requirement to disclose the incident's remediation status, whether it is ongoing, and whether data were compromised.[26]
- Removed a proposed requirement to disclose in a registrant's next periodic report when, to the extent known by management, multiple previously undisclosed, individually immaterial cybersecurity incidents became material in the aggregate.[27]
- Removed a proposed requirement to disclose the frequency of management-board discussions on cybersecurity (though, this may still be disclosed in certain circumstances) under Regulation S-K Item 106(c).[28]
- Removed the proposed amendment to Item 407 of Regulation S-K, which would have required disclosures about cybersecurity expertise, if any, of a registrant's board members.[29]

[24] *Id*. at 50-52.
[25] *Id*. at 30.
[26] *Id*. at 30.
[27] *Id*. at 47, 52.
[28] *Id*. at 69. Note, however, that some registrants may, depending on the context, include the frequency in which their board or board committee is informed about cybersecurity risks when describing their processes. *Id*.
[29] *Id.* at 83-85.

Contributors

Nickolas Andreacchi
ASSOCIATE

nickolas.andreacchi@wilmerhale.com
+1 617 526 6066

C. Alex Bahn
PARTNER

alex.bahn@wilmerhale.com
+1 202 663 6198

Lillian Brown
PARTNER

lillian.brown@wilmerhale.com
+1 202 663 6743

Meredith B. Cross
PARTNER

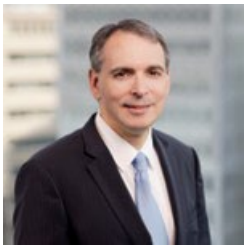
meredith.cross@wilmerhale.com
+1 212 295 6644

Amy M. Gopinathan
ASSOCIATE

amy.gopinathan@wilmerhale.com
+1 202 663 6761

Kirk J. Nahra
PARTNER

kirk.nahra@wilmerhale.com
+1 202 663 6128



Benjamin A. Powell
PARTNER

benjamin.powell@wilmerhale.com
+1 202 663 6770

Alan J. Wilson
COUNSEL

alan.wilson@wilmerhale.com
+1 202 663 6474

Jonathan Wolfman
PARTNER

jonathan.wolfman@wilmerhale.com
+1 617 526 6833