Press Release

SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

FOR IMMEDIATE RELEASE
2022-39

Washington D.C., March 9, 2022 — The Securities and Exchange Commission today proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

"Over the years, our disclosure regime has evolved to reflect evolving risks and investor needs," said SEC Chair Gary Gensler. "Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner. I am pleased to support this proposal because, if adopted, it would strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting."

The proposed amendments would require, among other things, current reporting about material cybersecurity incidents and periodic reporting to provide updates about previously reported cybersecurity incidents. The proposal also would require periodic reporting about a registrant's policies and procedures to identify and manage cybersecurity risks; the registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures. The proposal further would require annual reporting or certain proxy disclosure about the board of directors' cybersecurity expertise, if any.

The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification to investors of material cybersecurity incidents.

The proposing release will be published on SEC.gov and in the Federal Register. The comment period will remain open for 60 days following publication of the proposing release on the SEC's website or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.

###

Related Materials

- Proposed Rule
- Fact Sheet

FACT SHEET

Public Company Cybersecurity; Proposed Rules

The Securities and Exchange Commission proposed rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies ("registrants") that are subject to the reporting requirements of the Securities Exchange Act of 1934.

Specifically, the proposal would:

- Require current reporting about material cybersecurity incidents on Form 8-K;
- Require periodic disclosures regarding, among other things:
  - A registrant's policies and procedures to identify and manage cybersecurity risks;
  - Management's role in implementing cybersecurity policies and procedures;
  - Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and
  - Updates about previously reported material cybersecurity incidents; and
- Require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).

Background and Current Requirement

In 2011, the Division of Corporation Finance issued interpretive guidance providing the Division's views concerning registrants' existing disclosure obligations relating to cybersecurity risks and incidents. In 2018, the Commission issued interpretive guidance to reinforce and expand upon the 2011 staff guidance. The Commission addressed the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity. Although registrants' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since then, disclosure practices are inconsistent.

The proposed amendments are designed to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents. Consistent, comparable, and decision-useful disclosures would allow investors to evaluate registrants' exposure to cybersecurity risks and incidents as well as their ability to manage and mitigate those risks and incidents.

Incident Disclosure Proposed Amendments

The SEC proposed to:

- Amend Form 8-K to require registrants to disclose information about a material cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident;
- Add new Item 106(d) of Regulation S-K and Item 16J(d) of Form 20-F to require registrants to provide updated disclosure relating to previously disclosed cybersecurity incidents and to require disclosure, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate; and
- Amend Form 6-K to add "cybersecurity incidents" as a reporting topic.

Risk Management, Strategy, and Governance Disclosure

In addition to incident reporting, the SEC proposed to require enhanced and standardized disclosure on registrants' cybersecurity risk management, strategy, and governance. Specifically, the proposal would:

- Add Item 106 to Regulation S-K and Item 16J of Form 20-F to require a registrant to:
    - Describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity as part of its business strategy, financial planning, and capital allocation; and
    - Require disclosure about the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the registrant's cybersecurity policies, procedures, and strategies.
- Amend Item 407 of Regulation S-K and Form 20-F to require disclosure regarding board member cybersecurity expertise. Proposed Item 407(j) would require disclosure in annual reports and certain proxy filings if any member of the registrant's board of directors has expertise in cybersecurity, including the name(s) of any such director(s) and any detail necessary to fully describe the nature of the expertise.

Additional Information:

The public comment period will remain open for 60 days following publication of the proposing release on the SEC's website or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.