SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229, 232, 239, 240, and 249

[Release Nos. 33–11038; 34–94382; IC–34529; File No. S7–09–22]

RIN 3235–AM89

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission (''Commission'') is proposing rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are proposing amendments to require current reporting about material cybersecurity incidents. We are also proposing to require periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk. Additionally, the proposed rules would require registrants to provide updates about previously reported cybersecurity incidents in their periodic reports. Further, the proposed rules would require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (''Inline XBRL''). The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents.

DATES: Comments should be received on or before May 9, 2022.

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (*https://www.sec.gov/rules/submitcomments.htm*).
- Send an email to *rule-comment@sec.gov.* Please include File Number S7–09–22 on the subject line; or

Paper Comments

- Send paper comments to Vanessa A. Countryman, Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549–1090.

All submissions should refer to File Number S7–09–22. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method of submission. The Commission will post all comments on the Commission's website (*https://www.sec.gov/rules/proposed.shtml*). Comments also are available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Operating conditions may limit access to the Commission's public reference room. All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly.

Studies, memoranda, or other substantive items may be added by the Commission or staff to the comment file during this rulemaking. A notification of the inclusion in the comment file of any such materials will be made available on our website. To ensure direct electronic receipt of such notifications, sign up through the ''Stay Connected'' option at *www.sec.gov* to receive notifications by email.

FOR FURTHER INFORMATION CONTACT: Ian Greber-Raines, Special Counsel, Office of Rulemaking, at (202) 551–3460, Division of Corporation Finance; and, with respect to the application of the proposal to business development companies, David Joire, Senior Special Counsel, at (202) 551–6825 or *IMOCC@sec.gov,* Chief Counsel's Office, Division of Investment Management, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

SUPPLEMENTARY INFORMATION: We are proposing to amend or add the following rules and forms:

Commission reference		CFR citation (17 CFR)
Regulation S–K		17 CFR 229.10 through 229.1305.
	Items 106 and 407	§ 229.106 and § 229.407.
Regulation S–T		17 CFR 232.10 through 232.903.
	Rule 405	§ 232.405.
Securities Act of 1933 (''Securities Act'') [1]	Form S–3	§ 239.13.
	Form SF–3	§ 239.45.
	Rule 13a–11	§ 240.13a–11.
Securities Exchange Act of 1934 (''Exchange Act'') [2]	Rule 15d–11	§ 240.15d–11.
	Schedule 14A	§ 240.14a–101.
	Schedule 14C	§ 240.14c–101.
	Form 20–F	§ 249.220f.
	Form 6–K	§ 249.306.
	Form 8–K	§ 249.308.
	Form 10–Q	§ 249.308A.
	Form 10–K	§ 249.310.

Table of Contents

[1] 15 U.S.C. 77a *et seq.*

[2] 15 U.S.C. 78a *et seq.*

I. Background

Public company investors and other participants in the capital markets depend on companies' use of secure and reliable information systems to conduct their businesses. A significant and increasing amount of the world's economic activities occurs through digital technology and electronic communications.[3] In today's digitally connected world, cybersecurity threats and incidents pose an ongoing and escalating risk to public companies, investors, and market participants.[4] Cybersecurity risks have increased for a variety of reasons, including the digitalization of registrants' operations; [5] the prevalence of remote work, which has become even more widespread because of the COVID–19 pandemic; [6] the ability of cyber-criminals to monetize cybersecurity incidents, such as through ransomware, black markets for stolen data, and the use of crypto-assets for such transactions; [7] the growth of digital payments; [8] and increasing company reliance on third party service providers for information technology services, including cloud computing technology.[9] In particular, cybersecurity

[3] Bhaskar Chakravorti, Ajay Bhalla, & Ravi Shankar Chaturvedi, *Which Economies Showed the Most Digital Progress in 2020?,* Harv. Bus. Rev. (Dec. 18, 2020), *available at https://hbr.org/2020/12/which-economies-showed-the-most-digital-progress-in-2020. See Percentage of Business Conducted Online,* IBISWORLD, *https://www.ibisworld.com/us/bed/percentage-of-business-conducted-online/88090/* (last updated Jan. 13, 2022). *See also U.S. Department of Commerce, Bureau of Economic Analysis, Updated Digital Economy Estimates—June 2021, available at https://www.bea.gov/system/files/2021-06/DE%20June%202021%20update%20for%20web%20v3.pdf* (''The digital economy accounted for 9.6 percent ($2,051.6 billion) of current-dollar gross domestic product ($21,433.2 billion) in 2019, according to new estimates from BEA. When compared with traditional U.S. industries or sectors, the digital economy ranked just below the manufacturing sector[.]'').

[4] *See* Steve Morgan, *Cybercrime to Cost The World $10.5 Trillion Annually By 2025,* Cybercrime Magazine, (Nov. 13, 2020), *available at https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/*; Matt Powell, *11 Eye Opening Cyber Security Statistics for 2019,* CPO Magazine (June 25, 2019) *available at https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/* (The largest cybersecurity incidents involving public companies took place in the last ten years.); *see* Michael Hill and Dan Swinhoe, cso, The 15 biggest data breaches of the 21st century, *available at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html; see e.g.,* Commission Statement and Guidance on Public Company Cybersecurity Disclosures (''2018 Interpretive Release''), Release No. 33–10459 (Feb. 26, 2018) No. 33–10459 (Feb. 21, 2018) [83 FR 8166 Feb. 26, 2018], *available at https://www.sec.gov/rules/interp/2018/33-10459.pdf* (''Companies today rely on digital technology to conduct their business operations and engage with their customers, business partners, and other constituencies. In a digitally connected world, cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.'').

[5] *See The US Digital Trust Insights Snapshot,* PwC Research (June 2021), *available at https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/2021-digital-trust-insights/cyber-threat-landscape.html.*

[6] *See* Stephen Klemash and Jamie Smith, *What companies are disclosing about cybersecurity risk and oversight,* EY (Aug. 10, 2020), *available at https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight* (noting ''[w]ith the COVID–19-driven accelerated shift to digital business and massive, potentially permanent shifts to remote working, including virtual board and executive management meetings, cybersecurity risks are exponentially greater.''). *See Navigating Cyber 2021,* FS–ISAC, *available at https://www.fsisac.com/navigatingcyber2021-report. See also* Vikki Davis, *Combating the cybersecurity risks of working home,* Cyber Magazine (Dec. 2, 2021), *available at https://cybermagazine.com/cyber-security/combating-cybersecurity-risks-working-home. See also* Dave Burg, Mike Maddison, & Richard Watson, *Cybersecurity: How do you rise above the waves of a perfect storm?,* The EY Glob. Info. Sec. Survey (July 22, 2021), *available at https://www.ey.com/en_us/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm.* (in a survey of 1,000 senior cybersecurity leaders, the results indicated that 81% of those surveyed said that COVID–19 forced organizations to bypass cybersecurity processes.).

[7] *See Combating Ransomware: A Comprehensive Framework For Action: Key Recommendations from the Ransomware Task Force,* Inst. for Sec. & Tech. (Apr. 2021), *available at https://securityandtechnology.org/ransomwaretaskforce/report*; (''The explosion of ransomware as a lucrative criminal enterprise has been closely tied to the rise of Bitcoin and other cryptocurrencies, which use distributed ledgers, such as blockchain, to track transactions.''); *see* James Lewis, *Economic Impact of Cybercrime—No Slowing Down,* P. 4, CSIS (Feb. 2018) (''Monetization of stolen data, which has always been a problem for cybercriminals, seems to have become less difficult because of improvements in cybercrime black markets and the use of digital currencies.''). *But see* Avivah Litan, *Gartner Predicts Criminal Cryptocurrency Transactions Will Drop by 30% by 2024,* gartner (Jan. 14, 2022) *available at https://www.gartner.com/en/articles/gartner-predicts-criminal-cryptocurrency-transactions-will-drop-by-30-by-2024* (predicting that successful ransomware payments will drop in the near future because of a number of developments including the transparency behind the blockchain platforms that crypto tokens use). *See also* Jeff Benson, *Biden Administration Seeks to Expand Crypto Tracking to Fight Ransomware,* decrypt, *available at https://decrypt.co/72582/biden-administration-seeks-expand-crypto-tracking-fight-ransomware* (noting that law enforcement agencies are putting additional resources into crypto-asset tracking as ''the overwhelming majority of ransomware attackers demand Bitcoin.'').

[8] Sumathi Bala, *Rise in online payments spurs questions over cybersecurity and privacy,* CNBC (July 1, 2021), *available at https://www.cnbc.com/2021/07/01/new-digital-payments-spur-questions-over-consumer-privacy-security-.html* (''Threats over cyber security have become a growing concern as more people turn to online payments.''). *See also* Vaibhav Goel, Deepa Mahajan, Marie-Claude Nadeau, Owen Sperling, & Stephanie Yeh, *New trends in US consumer digital payments,* McKinsey & Company (Oct. 2021), *available at https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/new-trends-in-us-consumer-digital-payments.*

[9] *See The Cost of Third-Party Cybersecurity Risk Management,* Ponemon Institute LLC (Mar. 2019), *available at https://info.cybergrx.com/ponemon-report* (''Third-party breaches remain a dominant

Continued

incidents involving third party service provider vulnerabilities are becoming more frequent.[10] Additionally, cyber criminals are using increasingly sophisticated methods to execute their attacks.[11]

With an increase in the prevalence of cybersecurity incidents, there is an increased risk of the effect of cybersecurity incidents on the economy and registrants. Large scale cybersecurity attacks can have systemic effects on the economy as a whole, including serious effects on critical infrastructure and national security.[12] Public companies of all sizes and operating in all industries are susceptible to cybersecurity incidents that can stem from intentional or unintentional acts.[13] Additionally, senior management and boards of directors of public companies have become increasingly concerned about cybersecurity threats.[14] In a 2019 survey, chief executive officers of the largest 200 global companies rated '''national and corporate cybersecurity' as the number one threat to business growth and the international economy in the next 5 or 10 years.'' [15]

The cost to companies and their investors of cybersecurity incidents is rising and doing so at an increasing rate.[16] The types of costs and adverse consequences that companies may incur or experience as a result of a cybersecurity incident include the following:[17]

- Costs due to business interruption, decreases in production, and delays in product launches;
- Payments to meet ransom and other extortion demands;
- Remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;
- Increased cybersecurity protection costs, which may include increased insurance premiums and the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants;
- Lost revenues resulting from intellectual property theft and the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;
- Harm to employees and customers, violation of privacy laws, and reputational damage that adversely affects customer or investor confidence; and
- Damage to the company's competitiveness, stock price, and long-term shareholder value.

As indicated by the examples enumerated above, the potential costs and damage that can stem from a material cybersecurity incident are extensive. Many smaller companies have been targets of cybersecurity attacks so severe that the companies have gone out of business as a result.[18] These direct and indirect financial costs can negatively impact stock prices,[19] as well as short-term and long-term shareholder value. To mitigate the potential costs and damage that can result from a material cybersecurity incident, management and boards of directors may establish and maintain effective risk management strategies to address cybersecurity risks.[20]

Recent research suggests that cybersecurity is among the most critical governance-related issues for investors, especially U.S. investors.[21] Some

security challenge for organizations, with over 63% of breaches linked to a third party.''); *see Digital Transformation & Cyber Risk: What You Need to Know Stay Safe,* Ponemon Sullivan Privacy Report (June 2020), *available at https://ponemonsullivanreport.com/2020/07/digital-transformation-cyber-risk-what-you-need-to-know-to-stay-safe/* (although companies are increasingly reliant on third parties, ''63% of respondents say their organizations have difficulty ensuring there is a secure cloud environment.''). *See, e.g., Cost of Data Breach Report 2021,* IBM (July 2021), *available at https://www.ibm.com/security/data-breach* (finding 15% of the initial cybersecurity attack vectors were caused by cloud misconfiguration).

[10] *See Data Risk in the Third-Party Ecosystem: Second Annual Study,* Ponemon Institute LLC (Sept. 2017) *available at https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/sep2017/cs2017_0340.pdf* (noting that ''Data breaches caused by third parties are on the rise.''). *See e.g., The Cost of Third Party Cybersecurity Risk Management,* Ponemon Institute LLC (Mar. 2019), *available at https://www.cybergrx.com/resources/research-and-insights/ebooks-and-reports/the-cost-of-third-party-cybersecurity-risk-management* (''Over 53% of respondents have experienced a third-party data breach in the past 2 years at an average cost of $7.5 million.'').

[11] *See Cybersecurity: How do you rise above the waves of a perfect storm?, supra* note 6.

[12] *See* Cyber-Risk Oversight 2020, Key Principles and Practical Guidance for Corporate Boards (2020), nacd, *available at http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf* (''According to the Global Risks Report 2019, business leaders in advanced economies rank cyberattacks among their top concerns. A serious attack can destroy not only a company's financial health but also have systemic effects causing harm to the economy as a whole and even national security.''). *See also The Cost of Malicious Cyber Activity to the U.S. Economy* (Feb. 16, 2018), White H. Council of Econ. Advisers, *available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf* (''An attack have significant spillover effects to corporate partners, customers, and suppliers.'') and Testimony of Robert Kolasky, Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency (CISA), *Securing U.S. Surface Transportation from Cyber Attacks,* U.S. House of Representatives, Committee on Homeland Security (Feb. 26, 2019), *available at https://www.congress.gov/116/meeting/house/108931/witnesses/HHRG-116-HM07-Wstate-KolaskyB-20190226.pdf. See also Exec. Order No. 14028, Improving the Nation's Cybersecurity,* (May 12, 2021), 86 FR 26633, *available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.*

[13] *See Economic Report of the President: Together with The Annual Report of the Council of Economic Advisers,* (Mar. 2019), *available at https://www.govinfo.gov/content/pkg/ERP-2019/pdf/ERP-2019.pdf* (''Drawing on new data, we document that cyber vulnerabilities are quite prevalent—even in Fortune 500 companies with significant resources at their disposal.'').

[14] NACD, *Cyber-Risk Oversight2020, Key Principles and Practical Guidance for Corporate Boards, supra* note 12.

[15] *See EY CEO Imperative Study 2019,* July 2019, *available at https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/growth/ey-ceo-imperative-exec-summ-single-spread-final.pdf.*

[16] *See Cost of Data Breach Report 2021,* IBM Security (July 2021), *available at https://www.ibm.com/security/data-breach* (''The average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years.'').

[17] *See e.g., 2018 Interpretive Release*; and Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, & Rene M. Stulz, *Risk management, firm reputation, and the impact of successful cyberattacks on target firms,* 139 J. of Fin. Econ. at 747, 749 (2021).

[18] *See* Testimony of Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College, before the U.S. House of Representatives Committee on Small Business (Apr. 22, 2015), *available at http://docs.house.gov/meetings/SM/SM00/20150422/103276/HHRG-114-SM00-20150422-SD003-U4.pdf* (''Fifty percent of [small businesses] SMB's have been the victims of cyber attack and over 60 percent of those attacked go out of business. Often SMB's do not even know they have been attacked until it is too late.'').

[19] *See infra* note 101, section III.A.

[20] *See* NACD, *Cyber-Risk Oversight2020, Key Principles and Practical Guidance for Corporate Boards, supra* note 12.

[21] *2019 Responsible Investing Survey Key Findings,* RBC Glob. Asset Mgmt. (2019), *available at https://global.rbcgam.com/sitefiles/live/documents/pdf/rbc-gam-responsible-investing-survey-key-findings-2019.pdf.* This was a study developed by RBC Global Asset Management and BlueBay Asset Management LLP and distributed to a range of constituencies including institutional asset owners, consultants, clients, P&I Research Advisory Panel members, and members of the Pensions & Investment database. Study participants included individuals in Canada, Europe, Asia, and the United States. Two thirds of all respondents identified cybersecurity as an issue they were concerned about. The percentages were higher for the U.S., where out of all the environmental, social, and governance (''ESG'')-issues, the highest percentage of respondents ranked cybersecurity as the most concerning issue. *See also* J.P. Morgan Global Research, *Why is Cybersecurity Important to ESG Frameworks?,* J.P. Morgan Glob. Rsch. (Aug. 19, 2021), *available at https://www.jpmorgan.com/insights/research/why-is-cybersecurity-important-to-esg. See also Cyber security: Don't report on ESG without it* (2021), kpmg, *available at https://advisory.kpmg.us/articles/2021/cyber-security-report-on-esg.html.*

investors have been seeking information regarding registrants' cybersecurity risk management, strategy, and governance practices,[22] and there is evidence that the disclosure of cybersecurity incidents can affect both a registrant's reputation and its share price.[23] There may also be a positive correlation between a registrant's stock price and investments in certain cybersecurity technology.[24] Thus, 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.

We believe investors would benefit from more timely and consistent disclosure about material cybersecurity incidents, because of the potential impact that such incidents can have on the financial performance or position of a registrant. We also believe that investors would benefit from greater availability and comparability of disclosure by public companies across industries regarding their cybersecurity risk management, strategy, and governance practices in order to better assess whether and how companies are managing cybersecurity risks. The proposal reflects these policy goals.

Specifically, in this release, we are proposing to amend Form 8–K to require current disclosure of material cybersecurity incidents. We are also proposing to add new Item 106 of Regulation S–K that would require a registrant to: (1) Provide updated disclosure in periodic reports about previously reported cybersecurity incidents; (2) describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity risks as part of its business strategy, financial planning, and capital allocation; and (3) require disclosure about the board's oversight of cybersecurity risk, management's role in assessing and managing such risk, management's cybersecurity expertise, and management's role in implementing the registrant's cybersecurity policies, procedures, and strategies. We also are proposing to amend Item 407 of Regulation S–K to require disclosure of whether any member of the registrant's board has expertise in cybersecurity, and if so, the nature of such expertise.[25]

A. Existing Regulatory Framework and Interpretive Guidance Regarding Cybersecurity Disclosure

Although there are no disclosure requirements in Regulation S–K or S–X that explicitly refer to cybersecurity risks or incidents, in light of the increasing significance of cybersecurity incidents, over the past decade the Commission and staff have issued interpretive guidance concerning the application of existing disclosure and other requirements under the federal securities laws to cybersecurity risks and incidents. In 2011, the Division of Corporation Finance issued interpretive guidance (''2011 Staff Guidance''), providing the Division's views concerning operating companies' disclosure obligations relating to cybersecurity risks and incidents.[26]

In 2018, recognizing the ''the frequency, magnitude and cost of cybersecurity incidents,'' and the need for investors to be informed about material cybersecurity risks and incidents in a timely manner, the Commission issued interpretive guidance (''2018 Interpretive Release'') to assist operating companies in determining when they may be required to disclose information regarding cybersecurity risks and incidents under existing disclosure rules.[27] The 2018 Interpretive Release reinforced and expanded upon the 2011 Staff Guidance and also addressed the importance of cybersecurity policies and procedures, as well as the application of insider trading prohibitions in the context of cybersecurity.

Specifically, the 2018 Interpretive Release stated that companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure required in registration statements under the Securities Act and Exchange Act, as well as in periodic and current reports under the Exchange Act. The 2018 Interpretive Release identified the following existing provisions in Regulations S–K and S–X that may require disclosure about cybersecurity risks, governance, and incidents: [28]

- Item 105 of Regulation S–K (Risk Factors) [29]—the 2018 Interpretive Release sets forth issues for companies to consider in evaluating the need for cybersecurity risk factor disclosure, including risks arising in connection with acquisitions.
- Item 303 of Regulation S–K (Management's Discussion and Analysis of Financial Condition and Results of Operations) [30]—the 2018 Interpretive Release discusses how the costs of ongoing cybersecurity efforts, the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, can inform a company's management's discussion and analysis. The 2018 Interpretive Release describes a wide array of potential costs that may be associated with cybersecurity issues and incidents such as loss of intellectual property and reputational harm.
- Item 101 of Regulation S–K (Description of Business) [31]—the 2018 Interpretive Release notes that if cybersecurity incidents or risks materially affect a company's products,

[22] *See* Harvard Law School Forum on Corporate Governance Blog, posted by Steve W. Klemash, Jamie C. Smith, and Chuck Seets, *What Companies are Disclosing About Cybersecurity Risk and Oversight,* (posted Aug. 25, 2020) *available at https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight* (''Because the threat of a breach cannot be eliminated, some investors stressed that they are particularly interested in resiliency, including how (and how quickly) companies are detecting and mitigating cybersecurity incidents. Some are asking their portfolio companies about specific cybersecurity practices, such as whether the company has had an independent assessment of its cybersecurity program, and some are increasingly focusing on data privacy and whether companies are adequately identifying and addressing related consumer concerns and expanding regulatory requirements.'').

[23] *See* Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, & Rene M. Stulz, *Risk management, firm reputation, and the impact of successful cyberattacks on target firms,* 139 J. of Fin. Econ. at 747, 749 (2021); Georgios Spanos, and Lefteris Angelis, *The Impact of Information Security Events to the Stock Market: A Systematic Literature Review,* 58 Comput. & Sec. at 216, 226 (2016) (''Respectively, negative information security events, as the security breaches, have a negative impact to the stock price of the breached firms in the majority of the studies.'').

[24] *Id.*

[25] Proposed Item 407(j) of Regulation S–K.

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

[27] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33–10459 (Feb. 26, 2018) No. 33–10459 (Feb. 21, 2018) [83 FR 8166], *available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.* In 2018, the Commission also issued a Report of Investigation pursuant to Section 21(a) of the Exchange Act regarding certain cyber-related frauds perpetrated against public companies and related internal accounting controls requirements. The report cautioned that public companies subject to the internal accounting controls requirements of Exchange Act Section 13(b)(2)(B) should consider cyber threats when implementing their internal accounting controls. The report is based on SEC Enforcement Division investigations that focused on business email compromises in which perpetrators posed as company executives or vendors and used emails to dupe company personnel into sending large sums to bank accounts controlled by the perpetrators. *See Report of Investigation Pursuant to 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements,* SEC Release No. 34–84429 (Oct. 16, 2018).

[28] There are corresponding provisions in Form 20–F for foreign private issuers.

[29] *See also* Item 3.D of Form 20–F. Please note that Risk Factors was designated as Regulation S–K Item 503 at the time the 2018 Interpretive Release was issued.

[30] *See also* Item 5 of Form 20–F.

[31] *See also* Item 4.B of Form 20–F.

services, relationships with customers or suppliers, or competitive conditions, the company must provide appropriate disclosure.

- Item 103 of Regulation S–K (Legal Proceedings)—the 2018 Interpretive Release explains that this item may require disclosure about material pending legal proceedings that relate to cybersecurity issues.
- Item 407 of Regulation S–K (Corporate Governance) [32]—the 2018 Interpretive Release clarifies that a company must describe how the board administers its risk oversight function to the extent that cybersecurity risks are material to a company's business, including a description of the nature of the board's role in overseeing the management of such risks.
- Regulation S–X Financial Disclosures—the 2018 Interpretive Release notes the Commission's expectation that a company would design its financial reporting and control systems to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as that information becomes available.

The 2018 Interpretive Release also addresses the importance of a company's adoption of disclosure controls and procedures that cause the company to appropriately record, process, summarize, and report to investors material information related to cybersecurity risks and incidents.[33] In addition, the 2018 Interpretive Release reminds companies, their directors, officers, and other corporate insiders of the need to comply with insider trading laws in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches. The 2018 Interpretive Release further discusses disclosure obligations that companies may have under 17 CFR 243 (''Regulation FD'') in connection with cybersecurity matters. The guidance set forth in both the 2011 Staff Guidance and the 2018 Interpretive Release would remain in place if the Commission adopts the proposed rule amendments described in this release.

[32] This disclosure also is required by Item 7 of Schedule 14A.

[33] *See supra* note 4, 2018 Interpretive Release at 8167 (''Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.'').

B. Current Disclosure Practices

The majority of registrants reporting material cybersecurity incidents do so in a Form 8–K, press release, or periodic report. Although we are unable to determine the number of material cybersecurity incidents that either are not being disclosed or not being disclosed in a timely manner, the staff has observed certain cybersecurity incidents that were reported in the media but that were not disclosed in a registrant's filings. Further, the staff in the Division of Corporation Finance's review of Form 8–K filings, as well as Form 10–K and Form 20–F filings, has shown that the nature of the cybersecurity incident disclosure varies widely. In these filings, companies provide different levels of specificity regarding the cause, scope, impact, and materiality of cybersecurity incidents. For example, some companies provide a materiality analysis, disclose the estimated costs of an incident, discuss their engagement of cybersecurity professionals, and/or explain the remedial steps they have taken or are taking in response to a cybersecurity incident, while others do not provide such disclosure or provide much less detail in their disclosure on these topics.

The staff has also observed that, while the majority of registrants that are disclosing cybersecurity risks appear to be providing such disclosures in the risk factor section of their annual reports on Form 10–K, the disclosures are sometimes blended with other unrelated disclosures, which makes it more difficult for investors to locate, interpret, and analyze the information provided. Further, the staff has observed a divergence in these disclosures by industry and that, smaller reporting companies generally provide less cybersecurity disclosure as compared to larger registrants. One report noted a disconnect in which the industries experiencing the most high profile cybersecurity incidents provided disclosure with the ''least amount of information.'' [34] While cybersecurity risks and attacks may disproportionately affect certain industries at different times and in different ways, cybersecurity risks and threats may be dynamic; it is foreseeable and perhaps even predictable that malicious actors will adapt their strategies and target companies in any industry where there are perceived vulnerabilities.

Registrants' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since the issuance of the 2011 Staff Guidance and the 2018 Interpretive Release.[35] Yet, current reporting may contain insufficient detail [36] and the staff has observed that such reporting is inconsistent, may not be timely, and can be difficult to locate. We believe that investors would benefit from enhanced disclosure about registrants' cybersecurity incidents and cybersecurity risk management and governance practices, including if the registrant's board of directors has expertise in cybersecurity matters, and we are proposing rule amendments to enhance disclosure in those areas.

We welcome feedback and encourage interested parties to submit comments on any or all aspects of the proposed rule amendments. When commenting, it would be most helpful if you include the reasoning behind your position or recommendation.

II. Proposed Amendments

A. Overview

Cybersecurity risks and incidents can impact the financial performance or position of a company. Consistent, comparable, and decision-useful disclosures regarding a registrant's cybersecurity risk management, strategy, and governance practices, as well as a registrant's response to material cybersecurity incidents, would allow investors to understand such risks and incidents, evaluate a registrant's risk management and governance practices regarding those risks, and better inform their investment and voting decisions.

The proposed rules would require current and periodic reporting of

[34] Moody's Investors Service, Research Announcement, ''Cybersecurity disclosures vary greatly in high-risk industries,'' (Oct. 3, 2019), *available at https://www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854.*

[35] Stephen Klemash and Jamie Smith, *What companies are disclosing about cybersecurity risk and oversight,* EY, supra note 6 (EY researchers looked at cybersecurity-related disclosures in the proxy statements and Form 10–K filings for the 76 ''Fortune 100'' companies that filed those documents from 2018 through May 31, 2020. Their finding indicated that, ''[m]any companies are enhancing their cybersecurity disclosures, with modest increases across most of the disclosures tracked.'').

[36] One report notes ''the average public company's cyber disclosure contains insufficient detail for investors looking to evaluate its risk profile and to understand which remediation strategies, if any, it has implemented to control for the identified risks.'' NACD et al., *The State of Cyber-Risk Disclosures of Public Companies* at 3 (Mar. 2021) *available at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=71711.* This same report contends (and cites other sources that argue) that the 2018 Interpretive Release alone has not resulted in adequate disclosures to investors. *Id.* at 4.

material cybersecurity incidents. Additionally, we are proposing amendments that would require periodic disclosures about a registrant's policies and procedures to identify and manage cybersecurity risk, including the impact of cybersecurity risks on the registrant's business strategy; management's role and expertise in implementing the registrant's cybersecurity policies, procedures, and strategies; and the board of directors' oversight role, and cybersecurity expertise, if any.

Specifically, we are proposing to:

- Amend Form 8–K to add Item 1.05 to require registrants to disclose information about a cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident; [37]
- Amend Forms 10–Q and 10–K to require registrants to provide updated disclosure relating to previously disclosed cybersecurity incidents, as specified in proposed Item 106(d) of Regulation S–K. We also propose to amend these forms 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.[38]
- Amend Form 10–K to require disclosure specified in proposed Item 106 regarding:
  - A registrant's policies and procedures, if any, for identifying and managing cybersecurity risks; [39]
  - A registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks; [40] and
  - Management's role, and relevant expertise, in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies.[41]
- Amend Item 407 of Regulation S–K to require disclosure about if any member of the registrant's board of directors has cybersecurity expertise.[42]
- Amend Form 20–F to require foreign private issuers (''FPIs'') [43] to provide cybersecurity disclosures in their annual reports filed on that form that are consistent with the disclosure that we propose to require in the domestic forms;
- Amend Form 6–K to add ''cybersecurity incidents'' as a reporting topic; and
- Require that the proposed disclosures be provided in Inline XBRL.[44]

B. Reporting of Cybersecurity Incidents on Form 8–K

1. Overview of Proposed Item 1.05 of Form 8–K

There is growing concern that material cybersecurity incidents [45] are underreported [46] and that existing reporting may not be sufficiently timely.[47] We are proposing to address these concerns by requiring registrants to disclose material cybersecurity incidents in a current report on Form 8–K within four business days after the registrant determines that it has experienced a material cybersecurity incident.[48]

Specifically, we propose to amend Form 8–K by adding new Item 1.05 that would require a registrant to disclose the following information about a material cybersecurity incident, to the extent the information is known at the time of the Form 8–K filing:

- 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 of the incident on the registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incident.

We believe that this information would provide timely and relevant disclosure to investors and other market participants (such as financial analysts, investment advisers, and portfolio managers) and enable them to assess the possible effects of a material cybersecurity incident on the registrant, including any long-term and short-term financial effects or operational effects. While registrants should provide disclosure responsive to the enumerated items to the extent known at the time of filing of the Form 8–K, we would not expect a registrant to publicly disclose specific, 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.[49]

We believe that the proposed requirement to file an Item 1.05 Form 8–K within four business days after the registrant determines that it has experienced a material cybersecurity incident would significantly improve the timeliness of cybersecurity incident disclosures, as well as provide investors with more standardized and comparable disclosures.[50]

We are proposing that the trigger for an Item 1.05 Form 8–K is the date on which a registrant determines that a cybersecurity incident it has experienced is material, rather than the date of discovery of the incident, so as to focus the Form 8–K disclosure on

---

[37] Proposed Item 1.05.

[38] Proposed Item 106(d) of Regulation S–K.

[39] Proposed Item 106(b) of Regulation S–K.

[40] Proposed Item 106(c)(1) of Regulation S–K.

[41] Proposed Item 106(c)(2) of Regulation S–K.

[42] Proposed Item 407(j).

[43] An FPI is any foreign issuer other than a foreign government, except for an issuer that (1) has more than 50% of its outstanding voting securities held of record by U.S. residents; and (2) any of the following: (i) A majority of its officers or directors are citizens or residents of the U.S.; (ii) more than 50% of its assets are located in the U.S.; or (iii) its business is principally administered in the U.S. *See* 17 CFR 230.405. *See also* 17 CFR 240.3b–4(c).

[44] Proposed Rule 405 of Regulation S–T.

[45] *See infra* Section II.D.3 for a discussion on the proposed definition of ''cybersecurity incident.''

[46] *See New Study Reveals Cybercrime May Be Widely Underreported—Even When Laws Mandate Disclosure,* ISACA Press Release (June 3, 2019), *available at https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/new-study-reveals-cybercrime-may-be-widely-underreported-even-when-laws-mandate-disclosure. See also* Gerrit De Vynck, *Many ransomware attacks go unreported. The FBI and Congress want to change that.* Wash. Post (July 27, 2021), *available at https://www.washingtonpost.com/technology/2021/07/27/fbi-congress-ransomware-laws/* (quoting Eric Goldstein, executive assistant director at Cybersecurity & Infrastructure Security Agency (CISA), a federal agency created in 2018 to protect the U.S. from cyberattacks, as stating, ''[w]e believe that only about a quarter of ransomware intrusions are actually reported[.]'').

[47] *See also infra* section III.C(1)(a).

[48] As will be discussed in Section II.D, we propose to define the term ''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. We also propose to define the term ''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 a registrant's information to maintain or support the registrant's operations.'' The definitions of ''cybersecurity incident'' and ''information systems'' as proposed in Item 106 of Regulation S–K would also apply to such terms as used in proposed Item 1.05 of Form 8–K.

[49] *See also* 2018 Interpretive Release at Section II.A.1. Any material information not known or disclosable at the time of the Form 8–K filing would need to be updated in future periodic reports in response to proposed Item 106(d) of Regulation S–K. *See* discussion *infra* at Section II.C.1.

[50] If a triggering determination occurs within four business days before a registrant's filing of a Form 10–Q or Form 10–K, the Commission staff generally has not objected to the registrant satisfying its Form 8–K reporting obligation by including the disclosure in Item 5 (Other Information) of Part II of its Form 10–Q or Item 9B (Other Information) of its Form 10–K. *See* SEC Division of Corporation Finance, Exchange Act *Form 8-K Compliance and Disclosure Interpretations* (updated Dec. 22, 2017), Question 1, *available at https://www.sec.gov/divisions/corpfin/form8kfaq.htm.*

incidents that are material to investors. In some cases, the date of the registrant's materiality determination may coincide with the date of discovery of an incident, but in other cases the materiality determination will come after the discovery date. If we adopt the date of the materiality determination as the Form 8–K reporting trigger, as proposed, we expect registrants to be diligent in making a materiality determination in as prompt a manner as feasible. To address any concern that some registrants may delay making such a determination to avoid a disclosure obligation, Instruction 1 to proposed Item 1.05 states: ''a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident.''

What constitutes ''materiality'' for purposes of the proposed cybersecurity incidents disclosure would be consistent with that set out in the numerous cases addressing materiality in the securities laws, including: *TSC Industries, Inc.* v. *Northway, Inc.,*[51] *Basic, Inc.* v. *Levinson,*[52] and *Matrixx Initiatives, Inc.* v. *Siracusano.*[53] Information is material if ''there is a substantial likelihood that a reasonable shareholder would consider it important'' [54] in making an investment decision, or if it would have ''significantly altered the 'total mix' of information made available.'' [55] In articulating this materiality standard, the Supreme Court recognized that ''[d]oubts as to the critical nature'' of the relevant information ''will be commonplace.'' But ''particularly in view of the prophylactic purpose'' of the securities laws, and ''the fact that the content'' of the disclosure ''is within management's control, it is appropriate that these doubts be resolved in favor of those the statute is designed to protect,'' namely investors.[56]

A materiality analysis is not a mechanical exercise, nor should it be based solely on a quantitative analysis of a cybersecurity incident. Rather, registrants would need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors, to determine whether the incident is material. Even if the probability of an adverse consequence is relatively low, if the magnitude of the loss or liability is high, the incident may still be material; materiality ''depends on the significance the reasonable investor would place on'' the information.[57] Thus, under the proposed rules, when a cybersecurity incident occurs, registrants would need to carefully assess whether the incident is material in light of the specific circumstances presented by applying a well-reasoned, objective approach from a reasonable investor's perspective based on the total mix of information.

2. Examples of Cybersecurity Incidents That May Require Disclosure Pursuant to Proposed Item 1.05 of Form 8–K

The following is a non-exclusive list of examples of cybersecurity incidents [58] that may, if determined by the registrant to be material, trigger the proposed Item 1.05 disclosure requirement:

- 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 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.

3. Ongoing Investigations Regarding Cybersecurity Incidents

Proposed Item 1.05 would not provide for a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident. As the Commission stated in the 2018 Interpretive Release, while an ongoing investigation might affect the specifics in the registrant's disclosure, ''an ongoing internal or external investigation—which often can be lengthy—would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.'' [59] Additionally, any such delay provision 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. At the same time, we recognize that a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents. On balance, it is our current view that the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay.

Many states have laws that allow companies to delay providing public notice about a data breach incident or notifying certain constituencies of such an incident if law enforcement determines that notification will impede a civil or criminal investigation. A registrant may have obligations to report incidents at the state or federal level (to customers, consumer credit reporting entities, state or federal regulators and law enforcement agencies, etc.); those obligations are distinct from its obligations to disclose material information to its shareholders under the federal securities laws. To the extent that proposed Item 1.05 of Form 8–K would require disclosure in a situation in which a state law delay provision

[51] *TSC Indus.* v. *Northway,* 426 U.S. 438, 449 (1976).

[52] *Basic Inc.* v. *Levinson,* 485 U.S. 224, 232 (1988).

[53] 563 U.S. 27 (2011).

[54] *TSC Indus.* v. *Northway,* 426 U.S. at 449.

[55] *Id. See also* the definition of ''material'' in Securities Act Rule 405, 17 CFR 230.405; Exchange Act Rule 12b–2, 17 CFR 240.12b–2.

[56] *TSC Indus.* v. *Northway,* 426 U.S. at 448.

[57] *Basic Inc.* v. *Levinson,* 485 U.S. at 240.

[58] As discussed *infra* in Section II.D, we propose to define 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.'' We believe this term is sufficiently understood and broad enough to encompass incidents that could adversely affect a registrant's information systems or information residing therein, such as gaining access without authorization or by exceeding authorized access to such systems and information that could lead, for example, to the modification or destruction of systems and information. We also propose to define 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 a registrant's information to maintain or support the registrant's operations.'' The definitions of ''cybersecurity incident'' and ''information systems'' as proposed in Item 106 of Regulation S–K would also apply to such terms as used in proposed Item 1.05 of Form 8–K. *See infra* note 80.

[59] *See supra* note 33, 2018 Interpretive Release.

would excuse notification, there is a possibility a registrant would be required to disclose the incident on Form 8–K even though it could delay incident reporting under a particular state law. The proposed Form 8–K requirement would advance the objective of timely reporting of material cybersecurity incidents without the uncertainties of delay. It is critical to investor protection and well-functioning, orderly, and efficient markets that investors promptly receive information regarding material cybersecurity incidents.

4. Proposed Amendment to Form 6–K

FPIs are not required to file current reports on Form 8–K.[60] Instead, they are required to furnish on Form 6–K [61] copies of all information that the FPI: (i) Makes or is required to make public under the laws of its jurisdiction of incorporation, (ii) files, or is required to file under the rules of any stock exchange, or (iii) otherwise distributes to its security holders. We are proposing to amend General Instruction B of Form 6–K to reference material cybersecurity incidents among the items that may trigger a current report on Form 6–K. As with proposed Item 1.05 of Form 8–K, the proposed change to Form 6–K is intended to provide timely cybersecurity incident disclosure in a manner that is consistent with the general purpose and use of Form 6–K.

5. Proposed Amendments to the Eligibility Provisions of Form S–3 and Form SF–3 and Safe Harbor Provision in Exchange Act Rules 13a–11 and 15d–11

We are proposing to amend General Instruction I.A.3.(b) of Form S–3 and General Instruction I.A.2 of Form SF–3 to provide that an untimely filing on Form 8–K regarding new Item 1.05 would not result in loss of Form S–3 or Form SF–3 eligibility. Under our existing rules, the untimely filing on Form 8–K of certain specified items does not result in loss of Form S–3 or Form SF–3 eligibility, so long as Form 8–K reporting is current at the time the Form S–3 or SF–3 is filed. In the past, when we have adopted new disclosure requirements that differed from the traditional periodic reporting obligations of companies, we have acknowledged concerns about the potentially harsh consequences of the loss of Form S–3 or Form SF–3 eligibility, and addressed such concerns by specifying that untimely filing of Forms 8–K relating to certain topics would not result in the loss of Form S–3 or Form SF–3 eligibility.[62] For the same reason, we believe that it is appropriate to add proposed Item 1.05 to the list of Form 8–K items in General Instruction I.A.3.(b) of Form S–3 and General Instruction I.A.2 of Form SF–3.[63]

We are also proposing to amend Rules 13a–11(c) and 15d–11(c) under 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 under the Exchange Act.[64] In 2004, when the Commission adopted the limited safe harbor, the Commission noted its view that the safe harbor is appropriate if the triggering event for the Form 8–K requires management to make a rapid materiality determination.[65] While the registrant would need to file an Item 1.05 Form 8–K within four business days after the registrant determines that it has experienced a material cybersecurity incident, rather than within four business days after its discovery of the incident, we expect management to make a materiality determination about the incident as soon as reasonably practicable after its discovery of the incident.[66] In some cases, we expect that management would make a materiality determination coincident with discovering a cybersecurity incident and therefore file a Form 8–K very soon after the registrant experiences or discovers a cybersecurity incident. Therefore, we believe that it is appropriate to extend the safe harbor to this proposed new item.

Request for Comment

1. Would investors benefit from current reporting about material cybersecurity incidents on Form 8–K? Does the proposed Form 8–K disclosure requirement appropriately balance the informational needs of investors and the reporting burdens on registrants?

2. Would proposed Item 1.05 require an appropriate level of disclosure about a material cybersecurity incident? Would the proposed disclosures allow investors to understand the nature of the incident and its potential impact on the registrant, and make an informed investment decision? Should we modify or eliminate any of the specified disclosure items in proposed Item 1.05? Is there any additional information about a material cybersecurity incident that Item 1.05 should require?

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

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

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

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

[60] *See* Exchange Act Rules 13a–11 and 15d–11 [17 CFR 240.13a–11 and 15d–11].

[61] 17 CFR 249.306.

[62] *See* Selective Disclosure and Insider Trading, Release No. 33–7881 (Aug. 15, 2000) [65 FR 51715 (Aug. 24, 2000)]; *see also* Additional Form 8–K Disclosure Requirements and Acceleration of Filing Date, Release No. 33–8400 (Mar. 16, 2004) [69 FR 15593 (Mar. 25, 2004)] (the ''Additional Form 8–K Disclosure Release'').

[63] *See* Selective Disclosure and Insider Trading, Release No. 33–7881 (Aug. 15, 2000) [65 FR 51715]; Additional Form 8–K Disclosure Release.

[64] Rules 13a–11(c) and 15d–11(c) each provides that ''[n]o failure to file a report on Form 8–K that is required solely pursuant to Item 1.01, 1.02, 2.03, 2.04, 2.05, 2.06, 4.02(a), 5.02(e), or 6.03 of Form 8–K shall be deemed a violation of'' Section 10(b) of the Exchange Act or Rule 10b–5 thereunder.

[65] Additional Form 8–K Disclosure Release at 69 FR 15607.

[66] Instruction 1 to proposed Item 1.05 of Form 8–K.

timely disclosures to investors? What costs would registrants face in determining the extent of a potential conflict?

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

8. We are proposing to include an instruction that ''a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident.'' Is this instruction sufficient to mitigate the risk of a registrant delaying a materiality determination? Should we consider further guidance regarding the timing of a materiality determination? Should we, for example, suggest examples of timeframes that would (or would not), in most circumstances, be considered prompt?

9. Should certain registrants that would be within the scope of the proposed requirements, but that are subject to other cybersecurity-related regulations, or that would be included in the scope of the Commission's recently-proposed cybersecurity rules [67] for advisers and funds, if adopted, be excluded from the proposed requirements? For example, should the proposed Form 8–K reporting requirements or the other disclosure requirements described in this release, as applicable, exclude business development companies (''BDCs''),[68] or the publicly traded parent of an adviser?

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

11. We are proposing that registrants be required to file rather than permitted to furnish an Item 1.05 Form 8–K. Should we instead permit registrants to furnish an Item 1.05 Form 8–K, such that the Form 8–K would not be subject to liability under Section 18 of the Exchange Act unless the registrant specifically states that the information is to be considered ''filed'' or incorporates it by reference into a filing under the Securities Act or Exchange Act?

12. We note above a non-exclusive list of examples that would merit disclosure under Item 1.05 of Form 8–K covers some, but not all, types of material cybersecurity incidents. Are there additional examples we should address? Should we include a non-exclusive list of examples in Item 1.05 of Form 8–K?

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

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

C. Disclosure About Cybersecurity Incidents in Periodic Reports

1. Updates to Previously Filed Form 8–K Disclosure

Proposed Item 106(d)(1) of Regulation S–K would require registrants to disclose any material changes, additions, or updates to information required to be disclosed pursuant to Item 1.05 of Form 8–K in the registrant's quarterly report filed with the Commission on Form 10–Q or annual report filed with the Commission on Form 10–K for the period (the registrant's fourth fiscal quarter in the case of an annual report) in which the material change, addition, or update occurred.

We are proposing this requirement to balance the need for prompt and timely disclosure regarding material cybersecurity incidents with the fact that a registrant may not have complete information about a material cybersecurity incident at the time it determines the incident to be material. Proposed Item 106(d)(1) provides a means for investors to receive regular updates regarding the previously reported incident when and for so long as there are material changes, additions, or updates during a given reporting period. For example, after filing the initial Form 8–K disclosure, the registrant may become aware of additional material information about the scope of the incident and whether any data was stolen or altered; the proposed Item 106(d)(1) disclosure requirements would allow investors to stay informed of such developments.

The registrant also may be able to provide information about the effect of the previously reported cybersecurity incident on its operations as well as a description of remedial steps it has taken, or plans to take, in response to the incident that was not available at the time of the initial Form 8–K filing.[69] In order to assist registrants in developing updated incident disclosure in its periodic reports, proposed Item 106(d)(1) provides the following non-exclusive examples of the type of disclosure that should be provided, if applicable:

- Any material impact 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.

[67] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release No. 34–94197 (Feb. 9, 2022) [87 FR 13524 (Mar. 9, 2022)] (''Investment Management Cybersecurity Proposing Release''). In this release, the Commission proposed new rules and rule amendments that would require: (i) Registered investment advisers (''advisers'') and investment companies (''funds'') to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks; (ii) advisers to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients, to the Commission; (iii) advisers and funds to provide cyber-related disclosures to clients and investors; and (iv) advisers and funds to maintain certain records related to the proposed cybersecurity risk management obligations and the occurrence of cybersecurity incidents.

[68] For purposes of this release, the terms ''public companies,'' ''companies,'' and ''registrants,'' include issuers that are business development companies as defined in section 2(a)(48) of the Investment Company Act of 1940 (''Investment Company Act''), but not those investment companies registered under that Act.

[69] Notwithstanding proposed Item 106(d)(1), there may be situations where a registrant would need to file an amended Form 8–K to correct disclosure from the initial Item 1.05 Form 8–K, such as where that disclosure becomes inaccurate or materially misleading as a result of subsequent developments regarding the incident. For example, if the impact of the incident is determined after the initial Item 1.05 Form 8–K filing to be significantly more severe than previously disclosed, an amended Form 8–K may be required.

2. Disclosure of Cybersecurity Incidents That Have Become Material in the Aggregate

Proposed Item 106(d)(2) would require disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. Thus, registrants would need to analyze related cybersecurity incidents for materiality, both individually and in the aggregate. If such incidents become material in the aggregate, registrants would need to disclose: When the incidents were discovered and whether they are ongoing; a brief description of the nature and scope of such incidents; whether any data was stolen or altered; the impact of such incidents on the registrant's operations and the registrant's actions; and whether the registrant has remediated or is currently remediating the incidents.

While such incidents conceptually could take a variety of forms, an example would be where one malicious actor engages in a number of smaller but continuous cyber-attacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material, or both. Such incidents would need to be disclosed in the periodic report for the period in which a registrant has made a determination that they are material in the aggregate.

Request for Comment

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

16. Should we require a registrant to provide disclosure on Form 10–Q or Form 10–K when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate, as proposed? Alternatively, should we require a registrant to provide disclosure in Form 8–K, rather than in a periodic report, as proposed, when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate?

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

1. Risk Management and Strategy

Companies typically address significant risks to their businesses by developing risk management systems, which may include policies and procedures for identifying, assessing, and managing the risks. These policies and procedures may then be subject to oversight by a company's management and board.[70] Policies and procedures reasonably designed to provide oversight, risk assessments, and incident responses may be adopted to help prevent or mitigate cyber-attacks and potentially prevent future attacks. Staff in the Division of Corporation Finance has observed that most of the registrants that disclosed a cybersecurity incident in 2021 did not describe their cybersecurity risk oversight and related policies and procedures. Some of these registrants provided only general disclosures, such as a reference to cybersecurity as one of the risks overseen by the board or a board committee.

We are proposing Item 106(b) of Regulation S–K to require registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy. We believe that disclosure of the relevant policies and procedures, to the extent a registrant has established any, would benefit investors by providing greater transparency as to the registrant's strategies and actions to manage cybersecurity risks. For example, proposed disclosure about whether the registrant has a cybersecurity risk assessment program and undertakes activities designed to prevent, detect, and minimize effects of cybersecurity incidents can improve an investor's understanding of the registrant's cybersecurity risk profile. Given that a significant number of cybersecurity incidents pertain to third party service providers, the proposed rules would require disclosure concerning a registrant's selection and oversight of third-party entities as well.[71]

Additionally, cybersecurity risks may have an impact on a registrant's business strategy, financial outlook, or financial planning. Across industries, companies increasingly rely on information technology, collection of data, and use of digital payments as critical components of their business model and strategy. Their exposure to cybersecurity risks and previous cybersecurity incidents may affect these critical components, informing changes in their business model, financial condition, financial planning, and allocation of capital. For example, a company with a business model that relies highly on collecting and safeguarding sensitive and personally identifiable information from its customers may consider raising additional capital to invest in enhanced cybersecurity protection, improvements in its information security infrastructure, or employee cybersecurity training. Another company may examine the risks and decide that its business model should be adapted to minimize its collection of sensitive and personally identifiable information in order to reduce its risk exposure. These strategic decisions have implications for the company's financial planning and future financial performance. Disclosure about the impact of cybersecurity risks on business strategy would enable investors to assess whether companies will become more resilient or conversely, more vulnerable to cybersecurity risks in the future.

We also propose requiring disclosure of whether cybersecurity related risk and previous incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition. Investors would likely want to understand the financial impacts of cybersecurity risks and previous cybersecurity incidents in order to understand how these risks and incidents affect the company's financial performance or position, and thus the return on their investment. For example, a company that has previously experienced a cybersecurity incident may plan to provide compensation to consumers or it may anticipate regulatory fines or legal judgments as a result of the incident. These financial impacts would help investors understand the degree to which cybersecurity risks and incidents could affect the company's financial performance or position.

Proposed Item 106(b) would therefore require registrants to disclose its

[70] *See* Martin Lipton, Wachtell, Lipton, Rosen & Katz, *Spotlight on Boards 2018,* Harv. L. Sch. F. on Corp. Governance (May 31, 2018), *available at https://corpgov.law.harvard.edu/2018/05/31/spotlight-on-boards-2018* (one of the board's responsibilities is to, ''[o]versee and understand the corporation's risk management and compliance efforts and how risk is taken into account in the corporation's business decision-making; respond to red flags if and when they arise.'').

[71] *See* Stephen Klemash and Jamie Smith, *What companies are disclosing about cybersecurity risk and oversight,* EY, supra note 6 (''Around a third of the disclosed data breaches related to cyber attacks of third-party service providers.'').

policies and procedures, if it has any, to identify and manage 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. Specifically, proposed Item 106(b) of Regulation S–K would require disclosure, as applicable, of whether: [72]

- The registrant has a cybersecurity risk assessment program and if so, provide a description of such program;
- The registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program;
- The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider (including, but not limited to, those providers that have access to the registrant's customer and employee data), including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers;
- The registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents;
- The registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;
- Previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies;
- Cybersecurity related risk and incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition and if so, how; and
- Cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation and if so, how.

2. Governance

Disclosure regarding board oversight of a registrant's cybersecurity risk and the inclusion or exclusion of management from the oversight of cybersecurity risks and the implementation of related policies, procedures, and strategies impacts an investor's ability to understand how a registrant prepares for, prevents, or responds to cybersecurity incidents.[73] Accordingly, proposed Item 106(c) would require disclosure of a registrant's cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of such management, and its role in implementing the registrant's cybersecurity policies, procedures, and strategies.[74]

Specifically, as it pertains to the board's oversight of cybersecurity risk, disclosure required by proposed Item 106(c)(1) would include a discussion, as applicable, of the following: [75]

- 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.

This proposed disclosure about the board's oversight would inform investors about the role of the board in cybersecurity risk management, which may help inform their investment and voting decisions. Proposed Item 106(c)(1) would also reinforce the 2018 Interpretive Release, which states that the board's role in overseeing cybersecurity risks should be disclosed if ''cybersecurity risks are material to a company's business'' and that such disclosures should address how a board ''engages with management on cybersecurity issues'' and ''discharg[es] its [cybersecurity] risk oversight responsibility.'' [76]

Proposed Item 106(c)(2) would require a description of management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures, and strategies. This description would include, but not be limited to, the following information: [77]

- Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members;
- Whether the registrant has a designated chief information security officer,[78] or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart, and the relevant expertise [79] of any such persons;
- The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and
- Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

This proposed disclosure of how a registrant's management assesses and implements policies, procedures, and strategies to mitigate cybersecurity risks would be of importance to investors both as they understand how registrants are planning for cybersecurity risks and as they make decisions as to how best to allocate their capital.

3. Definitions

Proposed Item 106(a) defines the terms ''cybersecurity incident,'' ''cybersecurity threat,'' and ''information systems,'' as used in proposed Item 106 and proposed Form 8–K Item 1.05 as follows: [80]

[72] *See* proposed Item 106(b).

[73] *See* John F. Saverese et al., *Cybersecurity Oversight and Defense—A Board and Management Imperative,* Harv. L.Sch. F. on Corp. Governance (May 14, 2021), *available at https://corpgov.law.harvard.edu/2021/05/14/cybersecurity-oversight-and-defense-a-board-and-management-imperative/.*

[74] Proposed amendments to Form 10–K clarify that an asset-backed issuer (as defined in Item 1101 of Regulation AB) that does not have any executive officers or directors may omit the information required by 17 CFR 229.106(c) (Item 106(c) of Regulation S–K).

[75] *See* proposed Item 106(c)(1). In the case of a FPI with a two-tier board of directors, proposed Instruction 1 to Item 106(c) clarifies that the term ''board of directors'' means the supervisory or non-management board. In the case of a FPI meeting the requirements of 17 CFR 240.10A–3(c)(3), for purposes of proposed Item 106(c), the term, ''board of directors'' means the registrant's board of auditors (or similar body) or statutory auditors, as applicable.

[76] *See* 2018 Interpretive Release.

[77] *See* proposed Item 106(c)(2).

[78] The chief information security officer may be responsible for identifying and monitoring cybersecurity risks, communicating with senior management and the registrant's business units about acceptable risk levels, developing risk mitigation strategies, and implementing a security framework that protects the registrant's digital assets. *The Role of the CISO and the Digital Security Landscape,* isaca j. vol. 2, at 22, 23–29 (2019) *available at https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/the-role-of-the-ciso-and-the-digital-security-landscape.*

[79] Proposed Instruction 2 to Item 106(c) provides guidance that ''expertise'' in Item 106(c)(2)(i) and (ii) may include, for example: Prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.

[80] *See* proposed Item 106(a). These three terms are derived from a number of established sources. *See* Presidential Policy Directive—United States Cyber Incident Coordination (July 26, 2016) (''PPD–41''); 6 U.S.C. 1501 (2021); 44 U.S.C. 3502 (2021); 44 U.S.C. 3552 (2021); *see also* National Institute of Standards and Technology (NIST), Computer Security Resource Center Glossary (last visited Feb.

• *Cybersecurity incident* means 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.

• *Cybersecurity threat* means any potential occurrence that may result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

• *Information systems* means 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.

What constitutes a ''cybersecurity incident'' for purposes of our proposal should be construed broadly and may result from any one or more of the following: An accidental exposure of data, a deliberate action or activity to gain unauthorized access to systems or to steal or alter data, or other system compromises or data breaches.[81]

Request for Comment

17. Should we adopt Item 106(b) and (c) as proposed? Are there other aspects of a registrant's cybersecurity policies and procedures or governance that should be required to be disclosed under Item 106, to the extent that a registrant has any policies and procedures or governance? Conversely, should we exclude any of the proposed Item 106 disclosure requirements?

18. Are the proposed definitions of the terms ''cybersecurity incident,'' ''cybersecurity threat,'' and ''information systems,'' in Item 106(a) appropriate or should they be revised? Are there other terms used in the proposed amendments that we should define?

19. The proposed rule does not define ''cybersecurity.'' We could define the term to mean, for example: ''any action, step, or measure to detect, prevent, deter, mitigate, or address any cybersecurity threat or any potential cybersecurity threat.'' Would defining ''cybersecurity'' in proposed Item 106(a) be helpful? Why or why not? If defining this term would be helpful, is the definition provided above appropriate, or is there another definition that would better define ''cybersecurity''?

20. Should we require the registrant to specify whether any cybersecurity assessor, consultant, auditor, or other service that it relies on is through an internal function or through an external third-party service provider? Would such a disclosure be useful for investors?

21. As proposed, a registrant that has not established any cybersecurity policies or procedures would not have to explicitly state that this is the case. If applicable, should a registrant have to explicitly state that it has not established any cybersecurity policies and procedures?

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

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

24. Should we provide for delayed compliance or other transition provisions for proposed Item 106 for certain categories of registrants, such as smaller reporting companies, emerging growth companies, FPIs, or asset-backed securities issuers? Proposed Item 106(b), which would require companies to provide disclosures regarding existing policies and procedures for the identification and management of cybersecurity incidents, would be required in annual reports. Should the proposed Item 106(b) disclosures also be required in registration statements under the Securities Act and the Exchange Act?

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

E. Disclosure Regarding the Board of Directors' Cybersecurity Expertise

Cybersecurity is already among the top priorities of many boards of directors[82] and cybersecurity incidents and other risks are considered one of the largest threats to companies.[83] Accordingly, investors may find disclosure of whether any board members have cybersecurity expertise to be important as they consider their investment in the registrant as well as their votes on the election of directors of the registrant.

We propose to amend Item 407 of Regulation S–K by adding paragraph (j) to require disclosure about the cybersecurity expertise of members of the board of directors of the registrant, if any. If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise.[84]

The proposed requirements would build upon the existing disclosure requirements in Item 401(e) of Regulation S–K (business experience of directors) and Item 407(h) of Regulation

6, 2022), *available at https://csrc.nist.gov/glossary* (''NIST Glossary''). The proposed definitions also are consistent with proposed definitions in the Investment Management Cybersecurity Proposing Release. *See* Investment Management Cybersecurity Proposing Release at notes 27, 28, and 30. We believe the proposed terms are sufficiently precise for registrants to understand and use in connection with the proposed rules. Use of common terms is intended to facilitate compliance and reduce regulatory burdens. Using common terms and similar definitions with the Investment Management Cybersecurity Proposing Release along with other federal cybersecurity rulemakings is intended to facilitate compliance and reduce regulatory burdens.

[81] *See supra* Section II.B.2, for examples of cybersecurity incidents that may require disclosure pursuant to proposed Item 1.05 of Form 8–K.

[82] NACD, *2019–2020 NACD Public Company Governance Survey, available at https://corpgov.law.harvard.edu/wp-content/uploads/2020/01/2019-2020-Public-Company-Survey.pdf.*

[83] *See id.*

[84] Consistent with proposed Instruction 1 to Item 106(c), we are proposing an instruction to Item 407(j) to clarify that in the case of a FPI with a two-tier board of directors the term ''board of directors'' means the supervisory or non-management board. In the case of a FPI meeting the requirements of 17 CFR 240.10A–3(c)(3), for purposes of 407(j), the term, ''board of directors'' means the registrant's board of auditors (or similar body) or statutory auditors, as applicable. *See* proposed Instruction 2 to Item 407(j). Likewise, proposed General Instruction J to Form 10–K permits an asset-backed issuer that does not have any executive officers or directors to omit the Item 407 disclosure required by Form 10–K as these entities are generally passive pools of assets and are subject to substantially different reporting requirements than operating companies. Similarly, such entities would be permitted to omit the proposed Item 407(j) disclosure from Form 10–K under General Instruction J for the same reason.

S–K (board risk oversight). The proposed Item 407(j) disclosure would be required in a registrant's proxy or information statement when action is to be taken with respect to the election of directors, and in its Form 10–K.

Proposed Item 407(j) would not define what constitutes ''cybersecurity expertise,'' given that such expertise may cover different experiences, skills, and tasks. Proposed Item 407(j)(1)(ii) does, however, include the following non-exclusive list of criteria that a registrant should consider in reaching a determination on whether a director has expertise in cybersecurity:

- Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;
- Whether the director has obtained a certification or degree in cybersecurity; and
- Whether the director has 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.

Proposed Item 407(j)(2) would state that a person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including, without limitation, for purposes of Section 11 of the Securities Act (15 U.S.C. 77k),[85] as a result of being designated or identified as a director with expertise in cybersecurity pursuant to proposed Item 407(j).[86] This proposed safe harbor is intended to clarify that Item 407(j) would not impose on such person any duties, obligations, or liability that are greater than the duties, obligations, and liability imposed on such person as a member of the board of directors in the absence of such designation or identification.[87] This provision should alleviate such concerns for cybersecurity experts considering board service. Conversely, we do not intend for the identification of a cybersecurity expert on the board to decrease the duties and obligations or liability of other board members.[88]

Request for Comment

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

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

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

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

30. As proposed, Item 407(j)(1) includes a non-exclusive list of criteria that a company should consider in determining whether a director has expertise in cybersecurity. Are these factors for registrants to consider useful in determining cybersecurity expertise? Should the list be revised, eliminated, or supplemented?

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

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

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

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

35. Should certain categories of registrants, such as smaller reporting companies, emerging growth companies, or FPIs, be excluded from the proposed Item 407(j) disclosure requirement? How would any exclusion affect the ability of investors to assess the cybersecurity risk of a registrant or compare such risk among registrants?

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

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

F. Periodic Disclosure by Foreign Private Issuers

We propose to amend Form 20–F to add Item 16J that would require an FPI to include in its annual report on Form 20–F the same type of disclosure that we propose in Items 106 and 407(j) of Regulation S–K and that would be required in periodic reports filed by domestic registrants. One difference is that while domestic registrants would be required to include the proposed Item 407(j) disclosure about board expertise in both their annual reports and proxy or information statements, FPIs are not subject to Commission rules for proxy or information statement filings and thus, would only be required to include this disclosure in their annual reports.[89]

With respect to incident disclosure, where an FPI has previously reported an incident on Form 6–K, the proposed amendments would require an update regarding such incidents, consistent with proposed Item 106(d)(1) of Regulation S–K.[90] We are also proposing to amend Form 20–F to require FPIs to disclose on an annual basis information regarding any previously undisclosed material cybersecurity incidents that have occurred during the reporting period, including a series of previously undisclosed individually immaterial cybersecurity incidents that has become material in the aggregate.[91]

The Commission created Form 40–F in connection with its establishment of a multijurisdictional disclosure system (''MJDS''). This system generally

[85] 15 U.S.C. 77k.

[86] *See* proposed Item 407(j)(3)(i).

[87] *See* proposed Item 407(j)(3)(ii).

[88] *See* proposed Item 407(j)(3)(iii).

[89] Exchange Act Rule 3a12–3(b) [17 CFR 240.3a12–3(b)].

[90] *See* proposed Item 16J(d)(1).

[91] *See* proposed Item 16J(d)(2).

permits eligible Canadian FPIs to use Canadian disclosure standards and documents to satisfy the Commission's registration and disclosure requirements. Accordingly, we are not proposing prescriptive cybersecurity disclosure requirements for Form 40–F filers.

Request for Comment

38. Should we amend Form 20–F, as proposed to require disclosure regarding cybersecurity risk management and strategy, governance, and incidents? Additionally, should we amend Form 6–K, as proposed, to add ''cybersecurity incidents'' as a reporting topic? Are there unique considerations with respect to FPIs in these contexts?

39. We are not proposing any changes to Form 40–F. Should we instead require an MJDS issuer filing an annual report on Form 40–F to comply with the Commission's specific proposed cybersecurity-related disclosure requirements in the same manner as Form 10–K or Form 20–F filers?

G. Structured Data Requirements

We are proposing to require registrants to tag the information specified by Item 1.05 of Form 8–K and Items 106 and 407(j) of Regulation S–K in Inline XBRL in accordance with Rule 405 of Regulation S–T (17 CFR 232.405) and the EDGAR Filer Manual.[92] The proposed requirements would include block text tagging of narrative disclosures, as well as detail tagging of quantitative amounts disclosed within the narrative disclosures. Inline XBRL is both machine-readable and human-readable, which improves the quality and usability of XBRL data for investors.[93]

Requiring Inline XBRL tagging of the disclosures provided pursuant to these disclosure items would benefit investors by making the disclosures more readily available and easily accessible to investors, market participants, and others for aggregation, comparison, filtering, and other analysis, as compared to requiring a non-machine readable data language such as ASCII or HTML. This Inline XBRL tagging would enable automated extraction and analysis of the granular data required by the proposed rules, allowing investors and other market participants to more efficiently perform large-scale analysis and comparison of this information across registrants and time periods. For narrative disclosures, an Inline XBRL requirement would allow investors to extract and search for disclosures about cybersecurity incidents reported on Form 8–K, updated information about cybersecurity incidents reported in a registrant's periodic reports, a registrant's cybersecurity policies and procedures, management's role in assessing and managing cybersecurity risks, and the board of directors' oversight of cybersecurity risk and cybersecurity expertise rather than having to manually run searches for these disclosures through entire documents. The Inline XBRL requirement would also enable automatic comparison of these disclosures against prior periods, and targeted artificial intelligence/machine learning assessments of specific narrative disclosures rather than the entire unstructured document. At the same time, we do not expect the incremental compliance burden associated with tagging the proposed additional information to be unduly burdensome because registrants subject to the proposed tagging requirements are for the most part subject to similar Inline XBRL requirements in other Commission filings.

Request for Comment

40. Should we require registrants to tag the disclosures required by proposed Item 1.05 of Form 8–K and Items 106 and 407(j) of Regulation S–K in Inline XBRL, as proposed? Are there any changes we should make to ensure accurate and consistent tagging? If so, what changes should we make? Should we require registrants to use a different structured data language to tag these disclosures? If so, what structured data language should we require? Are there any registrants, such as smaller reporting companies, emerging growth companies, or FPIs that we should exempt from the tagging requirement?

General Request for Comment

We request and encourage any interested person to submit comments regarding the proposed rule amendments, specific issues discussed in this release, and other matters that may have an effect on the proposed rule amendments. With regard to any comments, we note that such comments are of particular assistance to our rulemaking initiative if accompanied by supporting data and analysis of the issues addressed in those comments.

III. Economic Analysis

A. Introduction

Cybersecurity threats and incidents continue to increase in prevalence and seriousness, posing an ongoing and escalating risk to public companies, investors, and other market participants.[94] The number of reported breaches disclosed by public companies has increased over the last decade, from 28 in 2011 to 144 in 2019 and 117 in 2020.[95] Although estimating the total cost of cybersecurity incidents is difficult, as many events may be unreported, some estimates put the total costs in the trillions of dollars per year in the U.S. alone.[96] The Council of Economic Advisers estimated that in 2016 the total cost of cybersecurity incidents was between $57 billion and $109 billion, or between 0.31 and 0.58 percent of U.S. GDP in that year.[97]

As described earlier, while cybersecurity incident disclosure has become more frequent since the issuance of the 2011 Staff Guidance and 2018 Interpretive Release, there is concern that material cybersecurity incidents are underreported.[98] For instance, the staff has observed that certain cybersecurity incidents were reported in the media but not disclosed in a registrant's filings.[99] Even when

[92] This tagging requirement would be implemented by including a cross-reference to Rule 405 of Regulation S–T in proposed Item 1.05 of Form 8–K and Items 106 and 407(j) of Regulation S–K, and by revising Rule 405(b) of Regulation S–T [17 CFR 232.405(b)] to include the listed disclosure Items. In conjunction with the EDGAR Filer Manual, Regulation S–T governs the electronic submission of documents filed with the Commission. Rule 405 of Regulation S–T specifically governs the scope and manner of disclosure tagging requirements for operating companies and investment companies, including the requirement in Rule 405(a)(3) to use Inline XBRL as the specific structured data language to use for tagging the disclosures.

[93] *See* Inline XBRL Filing of Tagged Data, Securities Act Release No. 10514 (June 28, 2018) [83 FR 40846 (Aug. 16, 2018)]. Inline XBRL allows filers to embed XBRL data directly into an HTML document, eliminating the need to tag a copy of the information in a separate XBRL exhibit. Inline XBRL is both human-readable and machine-readable for purposes of validation, aggregation, and analysis. *Id.* at 40851.

[94] Unless otherwise noted, when we discuss the economic effects of the proposed amendments on ''other market participants,'' we mean those market participants that typically provide services for investors and who rely on the information in registrant's filings (such as financial analysts, investment advisers, and portfolio managers).

[95] Audit Analytics, *Trends in Cybersecurity Breaches* (Mar. 2021) (stating that: ''[c]ybersecurity breaches can result in a litany of costs, such as investigations, legal fees, and remediation. There is also the risk of economic costs that directly impact financial performance, such as a reduction in revenue due to lost sales.'').

[96] *See* Cybersecurity and Infrastructure Security Agency, *Cost of a Cyber Incident: Systemic Review and Cross-Validation* (Oct. 26, 2020), *available at https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.*

[97] *See supra* note 12, The Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Feb. 2018).

[98] *See supra* section II.B and note 46. *See also infra* note 146, Amir et al. (2018) (providing evidence that companies underreport cyber-attacks).

[99] *See supra* section I.B.

disclosures about cybersecurity breaches are made, they may not be timely. According to Audit Analytics data, in 2020, it took on average 44 days for companies to discover breaches, and then in addition, it took an average of 53 days and a median of 37 days for companies to disclose a breach after its discovery.[100] Additionally, incident disclosure practices currently vary widely across registrants—some registrants disclose incidents through Form 8–K and some may disclose on a company website or in a press release. Because cybersecurity incidents can significantly impact companies' stock prices, delayed reporting results in mispricing of registrants' securities, harming investors.[101] Therefore, more timely and informative disclosure of a cybersecurity incident is needed for investors to assess an incident's impact and a registrant's ability to respond to the incident and to make more informed decisions.

Investors also need to better understand the growing cybersecurity risks registrants are facing and their ability to manage such risks in order to better value their securities. Executives, boards of directors, and investors are focused on this emerging risk. A 2019 survey of CEOs, boards of directors, and institutional investors found that they identified cybersecurity as the top global challenge for CEOs.[102] In 2021, a survey of audit committee members identified cybersecurity as the second highest risk that their audit committee would focus on in 2022, second only to financial reporting and internal controls.[103]

Disclosures about cybersecurity risk management, strategy, and governance are increasing, although they are not currently provided by all registrants. An analysis of disclosures by Fortune 100 companies found that disclosures of cybersecurity risk in proxy statements were found in 89 percent of filings in 2020, up from 79 percent in 2018, and disclosures of efforts to mitigate cybersecurity risk were found in 92 percent of proxy statements or 10–K Forms, up from 83 percent in 2018.[104]

As with incident reporting, there is a lack of uniformity in current reporting practice for cybersecurity risk management, strategy, and governance disclosure.[105] The relevant disclosures currently are made in varying sections of a registrant's periodic and current reports, such as in risk factors, in management's discussion and analysis, in a description of business and legal proceedings, or in financial statement disclosures, and are sometimes blended with other unrelated disclosures. The varied disclosure about both cybersecurity incidents and cybersecurity risk management, strategy, and governance makes it difficult for investors and other market participants to understand the cybersecurity risks that companies face and their preparedness for an attack, and to make comparisons across registrants.

To provide investors and other market participants with more timely, informative, and consistent disclosure about cybersecurity incidents, and cybersecurity risk management, strategy, and governance, we are proposing the following amendments.[106] Regarding incident reporting, we propose to: (1) Amend Form 8–K to add Item 1.05 to require registrants to disclose information about a cybersecurity incident within four business days following the registrant's determination that such an incident is material to the registrant; and (2) add new Item 106(d) of Regulation S–K to require registrants to provide updated disclosure in its periodic reports relating to previously disclosed incidents; and (3) amend Form 20–F and Form 6–K to require FPIs to provide cybersecurity disclosures consistent with the disclosure that we propose to require in the domestic forms.

For disclosures regarding cybersecurity risk management, strategy, and governance, we are proposing the following. First, we propose to amend Regulation S–K to require disclosure specified in proposed new Item 106(b) and (c) regarding: (1) A registrant's policies and procedures if any, for identifying and managing cybersecurity risks, (2) a registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity-related issues, and (3) management's role and expertise in assessing and managing cybersecurity risks and implementing related policies, procedures and strategies. Second, we propose to amend Item 407 of Regulation S–K to require disclosure about cybersecurity expertise of any member of the board.

The discussion below addresses the potential economic effects of the proposed amendments, including the likely benefits and costs, as well as the likely effects on efficiency, competition, and capital formation.[107] At the outset, we note that, where possible, we have attempted to quantify the benefits, costs, and effects on efficiency, competition, and capital formation expected to result from the proposed amendments. In many cases, however, we are unable to quantify the potential economic effects because we lack information necessary to provide a reasonable estimate. Where we are unable to quantify the economic effects of the proposed amendments, we provide a qualitative assessment of the potential effects and encourage commenters to provide data and information that would help quantify the benefits, costs, and the potential impacts of the proposed amendments on efficiency, competition, and capital formation.

B. Economic Baseline

1. Current Regulatory Framework

To assess the economic impact of the proposed rules, the Commission is using as its baseline the existing regulatory framework for cybersecurity disclosure. As discussed in Section I, although a number of rules and regulations impose an obligation on companies to disclose cybersecurity risks and incidents in certain circumstances, the Commission's regulations currently do not explicitly address cybersecurity.

In 2011, the Division of Corporation Finance issued interpretive guidance providing the Division's views concerning operating companies' disclosure obligations relating to cybersecurity risks and incidents.[108] The 2011 Staff Guidance provided an overview of existing specific disclosure obligations that may require a discussion of cybersecurity risks and

[100] *See supra* note 95 (''Audit Analytics'').

[101] *See infra* note 133.

[102] *See supra* note 15, *EY CEO Imperative Study* (2019). The Ernst & Young survey consisted of interviewing 200 global CEOs amongst the Forbes Global 2000 and Forbes largest private companies as well as interviewing 100 senior investors from global firms that had managed at least $100 billion in assets.

[103] *See* Center for Audit Quality, *Audit Committee Practices Report: Common Threads Across Audit Committees* (Jan. 2022), *available at https://www.thecaq.org/2022-ac-practices-report/.*

[104] *See* Jamie Smith, *How Cybersecurity Risk Disclosures and Oversight are Evolving in 2021,* EY Center for Board Matters (Oct. 5, 2021), *available at https://www.ey.com/en_us/board-matters/cybersecurity-risk-disclosures-and-oversight.*

[105] *See supra* section I.

[106] *See supra* section II.

[107] Section 2(b) of the Securities Act [15 U.S.C. 77b(b)] and Section 3(f) of the Exchange Act [15 U.S.C. 78c(f)] directs the Commission, when engaging in rulemaking where it is required to consider or determine whether an action is necessary or appropriate in the public interest, to consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation. Further, Section 23(a)(2) of the Exchange Act (15 U.S.C. 78w(a)(2)) requires the Commission, when making rules under the Exchange Act, to consider the impact that the rules would have on competition, and prohibits the Commission from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the Exchange Act.

[108] *See supra* section I.A and note 26.

cybersecurity incidents, along with examples of potential disclosures.[109] Building on the 2011 Staff Guidance, the Commission issued the 2018 Interpretive Release to assist operating companies in preparing disclosure about cybersecurity risks and incidents under existing disclosure rules.[110] In the 2018 Interpretive Release, the Commission instructed companies to provide timely and ongoing information in periodic reports (Form 10–Q, Form 10–K, and Form 20–F) about material cybersecurity risks and incidents that trigger disclosure obligations. Additionally, the 2018 Interpretive Release encouraged companies to continue to use current reports (Form 8–K or Form 6–K) to disclose material information promptly, including disclosure pertaining to cybersecurity matters. Further, the 2018 Interpretive Release noted that to the extent cybersecurity risks are material to a company's business, the Commission believes that the required disclosure of the company's risk oversight should include the nature of the board's role in overseeing the management of that cybersecurity risk. The 2018 Interpretive Release also stated that a company's controls and procedures should enable them to, among other things, identify cybersecurity risks and incidents and make timely disclosures regarding such risks and incidents. Finally, the 2018 Interpretive Release highlighted the importance of insider trading prohibitions and the need to refrain from making selective disclosures of cybersecurity risks or incidents.

Companies currently may also be subject to other cybersecurity incident disclosure requirements adopted by various industry regulators and contractual counterparties. For example, federal contractors may be required to monitor and report cybersecurity incidents and breaches or face liability under the False Claims Act.[111] The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities and their business associates to provide notification following a breach of unsecured protected health information.[112] Similar rules require vendors of personal health records and related entities to report data breaches to affected individuals and the Federal Trade Commission.[113] All 50 states have data breach laws that require businesses to notify individuals of security breaches involving their personally identifiable information.[114] There are other rules that companies must follow in international jurisdictions that are similar in scope to the proposed rules. For example, in the European Union, the General Data Protection Regulation mandates disclosure of cybersecurity breaches.[115] All of the aforementioned data breach disclosure requirements may cover some of the material incidents that companies would need to report under the proposed amendments, but not all incidents. Additionally, the timeliness and public reporting requirements of these requirements vary, making it difficult for investors and other market participants to be alerted to the breaches, and to be provided with an adequate understanding of the impact of such incidents to registrants.

Some companies are also subject to other mandates to fulfill a basic level of cybersecurity risk management, strategy, and governance. For instance, government contractors may be subject to the Federal Information Security Modernization Act, and use the National Institute of Standards and Technology framework to manage information and privacy risks.[116] Financial institutions may be subject to the Federal Trade Commission's Standards for Safeguarding Customer Information Rule, requiring an information security program and a qualified individual to oversee the security program and to provide periodic reports to a company's board of directors or equivalent governing body.[117] Under HIPAA regulations, covered entities are also subject to rules that require protection against reasonably anticipated threats to electronic protected health information.[118] International jurisdictions also have cybersecurity risk mitigation measures, for example, the GDPR requires basic cybersecurity risk mitigation measures and has governance requirements.[119] These various requirements have varying standards and requirements for reporting cybersecurity risk management, strategy, and governance, and may not provide investors with clear and comparable disclosure regarding how a particular registrant manages its cybersecurity risk profile.

2. Affected Parties

The proposed new disclosure requirements would apply to various filings, including current reports, periodic reports, and certain proxy statements filed with the Commission. Thus, the parties that are likely to be affected by the proposed rules include investors, registrants, other market participants that use the information in these filings (such as financial analysts, investment advisers, and portfolio managers) and external stakeholders such as consumers and other companies in the same industry as affected firms.

We expect the proposed rules to affect all companies with relevant disclosure obligations on Forms 10–K, 10–Q, 20–F, 8–K, or 6–K, and proxy statements. This includes approximately 7,848 companies filing on domestic forms and 973 FPIs filing on foreign forms based on all companies that filed such forms or an amendment thereto during calendar year 2020.[120]

Our textual analysis [121] of all calendar year 2020 Form 10–K filings and amendments (7,683) reveals that out of 6,634 domestic filers approximately 64% (4,272) of them made any cybersecurity-related disclosures. The filers' average size in terms of total assets and market capitalization was

[109] *Id.*

[110] *See supra* section I.A and note 27.

[111] *See* Department of Justice, Office of Public Affairs, *Justice News: Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative,* (Oct. 6, 2021), *available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative; see, e.g.,* FAR 52.239–1 (requiring contractors to ''immediately'' notify the federal government if they become aware of ''new or unanticipated threats or hazards . . . or if existing safeguards have ceased to function'').

[112] *See* 45 CFR 164.400–164.414 (Notification in the Case of Breach of Unsecured Protected Health Information).

[113] *See* 16 CFR 318 (Health Breach Notification Rule).

[114] Note that there are carve outs to these rules, and not every company may fall under any particular rule. *See Security Breach Notification Laws,* National Conference of State Legislatures (Jan. 17, 2022), *available at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.*

[115] *See* Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), arts. 33 (Notification of a personal data breach to the supervisory authority), 34 (Communication of a personal data breach to the data subject), 2016 O.J. (L 119) 1 (''GDPR'').

[116] *See NIST Risk Management Framework,* NIST (updated Jan. 31, 2022), *available at https://csrc.nist.gov/projects/risk-management/fisma-background.*

[117] *See* 16 CFR 314.

[118] *See* 45 CFR 164 (Security and Privacy).

[119] *See supra* note 115, GDPR, § 32, § 37.

[120] Estimates of affected registrants here are based on the number of unique CIKs with at least one periodic report, current report, proxy filing, or an amendment to one of the three filed in calendar year 2020.

[121] In performing this analysis, staff executed a combination of computer program-based keyword (and combination of key words) searches followed by manual review to classify disclosures by location within the document. This analysis covered 7,683 Forms 10–K and 10–K/A filed in calendar year 2020 by 6,634 registrants as identified by unique CIK.

approximately $14.1 billion and $7.5 billion, respectively.[122] By comparison, the average size of domestic annual report filers that did not make any cyber disclosures was $892.6 million and $2.2 billion in terms of total assets and market capitalization, respectively. However, the average size of all baseline affected filers was approximately $14.1 billion and $5.6 billion in total assets and market capitalization respectively.

The nature of these disclosures is summarized in the table below, which reports the relative frequency of cyber-related disclosures by location within the annual report conditional on a report having at least one discussion of cybersecurity. We note that the average number of reporting locations for registrants making cybersecurity-related disclosures on the annual report is 1.5, and registrants making cybersecurity-related disclosures often only did so in one section of the annual report (64%). However, many annual reports featured cybersecurity discussions in more than one section: 25% had disclosures in 2 sections, 7% in 3 sections, and 1% in 5 or more sections. Because of this, the percentages in Table 1 sum to greater than 100%.

TABLE 1—INCIDENCE OF CYBERSECURITY-RELATED DISCLOSURES BY 10–K LOCATION [a]

Disclosure location	Item description	Percentage
Item 1A	Risk Factors	94.3
Item 1	Description of Business *	20.5
PSLRA	Cautionary Language regarding Forward Looking Statements	16.3
Item 7	Management's Discussion and Analysis *	10.0
Item 10	Directors, Executive Officers and Corporate Governance	3.4
Item 8	Financial Statements and Supplementary Data	2.8
	Exhibits (attached)	0.9
Item 11	Executive Compensation	0.4
Item 15	Exhibits, Financial Statement Schedules	0.4
Item 2	Properties	0.3
Item 3	Legal Proceedings	0.3
Item 9	Changes in and Disagreements with Accountants on Accounting and Financial Disclosure *	0.2
Item 13	Certain Relationships and Related Transactions, and Director Independence	0.2
Item 6	Selected Financial Data	0.2
Item 5	Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities.	0.1
Item 4	Mine Safety Disclosures	0.1
Item 14	Principal Accountant Fees and Services	0.1
Item 12	Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters.	0.0

[a] Because of heterogeneity in registrants' labeling of sections, Items other than 1A are grouped only at the numeric level. An asterisk in the table denotes that the identified Item may contain disclosures located in a more specific subsection. Item 1, for instance, includes Item 1B disclosures; Item 7 includes 7A; and Item 9 includes 9A, 9B, and 9C.

As presented in Table 1, approximately 94% (4,029) of Form 10–K or amendment filers that provided any cyber-related disclosures included discussion of cybersecurity as a material risk factor in Item 1A.

We further estimate that, in 2020, approximately 603 domestic companies reported having a director on their board with cybersecurity experience or expertise. This estimate is based on a review of cybersecurity disclosures by registrants that filed either a Form 10–K or an amended Form 10–K in 2020 that included cybersecurity-related language in their Item 10 (Directors and Executive Officers of the Registrant) discussion or provided similar disclosures in a proxy filing instead.[123]

Finally, there were a total of 74,098 Form 8–K filings in 2020, involving 7,021 filers, out of which 40 filings reported material cybersecurity incidents. Similarly, there were a total of 23,373 Form 6–K filings in 2020, involving 979 filers, out of which 27 filings reported material cybersecurity incidents. Filers of annual, quarterly, or current reports (Forms 10–K, 10–Q, 20–F, 8–K, or 6–K) including a cybersecurity discussion in any form included 104 business development companies.

C. Potential Benefits and Costs of the Proposed Amendments

We have considered the potential benefits and costs associated with the proposed amendments. The proposed rules would benefit investors and other market participants by providing more timely and informative disclosures relating to cybersecurity incidents and cybersecurity risk management, strategy, and governance, facilitating investor decision-making and reducing information asymmetry in the market. The proposed amendments also would entail costs. For instance, in addition to the costs of providing the disclosure itself, more detailed disclosure could potentially increase the vulnerability of registrants and the risk of future attacks. A discussion of the anticipated economic costs and benefits of the proposed amendments is set forth in more detail below. We first discuss benefits to investors (and other market participants, such as financial analysts, investment advisers, and portfolio managers) and registrants. We subsequently discuss costs to investors and registrants. We conclude with a discussion of indirect economic effects on registrants and external stakeholders, such as consumers, and companies in the same industry with registrants or those facing similar cybersecurity threats.

We also expect the proposed amendments to affect compliance burdens. The quantitative estimates of changes in those burdens for purposes of the Paperwork Reduction Act of 1995 (''PRA'') are further discussed in Section [IV] below. For purposes of the PRA, we estimate that the proposed amendments would result in an increase of 2,000 and

[122] Market capitalization averages are estimated as of end of calendar year 2020. Total Asset averages are estimated from the value for the most recently completed fiscal year reported by a registrant by year end 2020.

[123] Based on manual review of the total of 15,565 proxy filings filed in 2020 and the 1,600 of them that mentioned cybersecurity.

180 burden hours from the increase in the number Form 8–K and Form 6–K filings respectively.[124] In addition, the estimated increase in the paperwork burden as a result of the proposed amendments for Form 10–Q, Form 10–K, Form 20–F, Schedule 14A, and Schedule 14C would be 3,000 hours, 132,576 hours, 12,028.50 hours, 3,900 hours, and 342 hours respectively.[125]

1. Benefits

Investors would be the main beneficiaries from the enhanced disclosure of both cybersecurity incidents and cybersecurity risk management, strategy, and governance as a result of the proposed amendments. Specifically, investors would benefit because: (1) More informative and timely disclosure would reduce mispricing of securities in the market and facilitate their decision making; and (2) more uniform and comparable disclosures would lower search costs and information processing costs. Other market participants that rely on financial statement information to provide services to investors, such as financial analysts, investment advisers, and portfolio managers, could also benefit. Registrants could benefit, because the enhanced disclosure as a result of the proposed amendments could reduce information asymmetry and potentially lower registrants' cost of capital.

a. Benefits to Investors

(i) More Informative and More Timely Disclosure

More informative and timely disclosures would reduce mispricing of securities in the market and facilitate investor decision making. Information benefits would result from both types of disclosure,[126] and timeliness benefits would result from the proposed cybersecurity incident disclosure.

The proposed amendments would provide more informative disclosures related to cybersecurity incidents and cybersecurity risk management, strategy, and governance compared to the current disclosure framework, benefiting investors. The increase in disclosure would allow investors to better understand a registrant's cybersecurity risks and ability to manage such risks, and thereby make more informed investment decisions. As discussed in Section I, currently, there are no disclosure requirements that explicitly refer to cybersecurity risks or incidents. While existing disclosure requirements may apply to material cybersecurity incidents and various cybersecurity risks and mitigation efforts, as highlighted in the 2011 Staff Guidance and the 2018 Interpretive Release, the existing disclosure requirements are more general in nature, and the resulting disclosures have not been consistently sufficient or necessarily informative.

Specifically, regarding incident reporting, there is concern that material cybersecurity incidents are underreported,[127] and staff has observed that certain cybersecurity incidents were reported in the media but not disclosed in a registrant's filings.[128] Even when registrants have filed Form 8–K to report an incident, the Form 8–K did not necessarily state whether or not the incident was material, and in some cases, the Form 8–K stated that the incident was immaterial.[129] By requiring registrants to disclose material cybersecurity incidents in a current report and disclose any material changes, additions, or updates in a periodic report, the proposed amendments could elicit more incident reporting. Because the proposed incident disclosure requirements also specify that registrants would disclose information such as when the incident was discovered, and the nature and scope of the incident, they could also result in more informative incident reporting.

Similarly, the proposed disclosure about cybersecurity risk management, strategy, and governance would include a number of specific items that registrants must disclose. For instance, the proposed rules would require disclosure regarding a registrant's policies and procedures for identifying and managing cybersecurity risks.[130] The proposed rules would also require disclosure concerning whether and how cybersecurity considerations affect a registrant's selection and oversight of third-party service providers because a significant number of cybersecurity incidents pertain to third party service providers.[131] As a result, the proposed rules related to risk management, strategy, and governance could also lead to more informative disclosure to investors.

We anticipate the proposed cybersecurity incident reporting would also lead to more timely disclosure to investors. As discussed above, currently, it could take months for registrants to disclose a material cybersecurity incident after its discovery.[132] The proposed amendments would require these incidents to be disclosed in a current report on Form 8–K within four business days after the registrant determines that it has experienced a material cybersecurity incident.

More informative and timely disclosure as a result of the proposed amendments would benefit investors because the enhanced disclosure could allow them to better understand the impact of a cybersecurity incident on the registrant, the risk a registrant is facing and its ability to manage the risk. Such information is relevant to the valuation of registrants' securities and thereby investors' decision making. It is well documented in the academic literature that the market reacts negatively to announcements of cybersecurity incidents. For example, one study finds a significant mean cumulative abnormal return of –0.84% in the three days following cyberattack announcements, which, according to the study, translates into an average value loss of $495 million per attack.[133] Another study finds that firms with higher exposure to cybersecurity risk have a higher cost of capital, suggesting

[124] *See infra* section IV.

[125] *Id.*

[126] Throughout this section, we use the term ''both types of disclosure'' to refer to the disclosure of (1) cybersecurity incidents and (2) cybersecurity risk management, strategy, and governance.

[127] *See supra* section II.B and note 46.

[128] *See supra* section I.B.

[129] Based on staff analysis of the current and periodic reports in 2021 for companies identified by as having been affected by a cybersecurity incident.

[130] *See supra* section II.D.

[131] *See supra* section II.D.

[132] *See supra* note 95, section III.A.

[133] *See* Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M. Stulz, *Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms,* 139 (3) J. of Fin. Econ. 721, 719–749 (2021). *See also* Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou, *The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?,* 19 (1) J. of Comput. Sec. 33, 33–56 (2011) (finding ''the impact of the broad class of information security breaches on stock market returns of firms is significant''); *see also* Georgios Spanos and Lefteris Angelis, *The Impact of Information Security Events to the Stock Market: A Systematic Literature Review,* 58 Comput. & Sec. 216–229 (2016) (documenting that the majority (75.6%) of the studies the paper reviewed report statistical significance of the impact of security events to the stock prices of firms). *But see* Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou, *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market,* 11 (3) J. of Comput. Sec. 432, 431–448 (2003) (while finding limited evidence of an overall negative stock market reaction to public announcements of information security breaches, they also find ''the nature of the breach affects this result'', and ''a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information''; they thus conclude that ''stock market participants appear to discriminate across types of breaches when assessing their economic impact on affected firms'').

that this risk is important to investors.[134] Therefore, whether a registrant is prepared for cybersecurity risks and has adequate cybersecurity risk management, strategy, and governance measures in place to reduce the likelihood of future incidents are important information for investors and the market. Delayed or incomplete reporting of cybersecurity incidents and risks could lead to mispricing of the securities and information asymmetry in the market, harming investors.

In addition, the mispricing resulting from delayed or limited disclosure could be exploited by the malicious actors who caused a cybersecurity incident, or those who could access and trade on material information stolen during a cybersecurity incident, causing further harm to investors.[135] Malicious actors may trade ahead of an announcement of a data breach that they caused or pilfer material information to trade on ahead of company announcements. Trading on undisclosed cybersecurity information is particularly pernicious, because profits generated from this type of trading would provide incentives for malicious actors to ''create'' more incidents and proprietary information to trade on.[136] More informative and timely disclosure as a result of the proposed amendments would reduce mispricing and information asymmetry, and thereby reduce opportunities for malicious actors to exploit the mispricing, all of which would enhance investor protection.

Overall, we believe enhanced disclosure as a result of the proposed amendments could benefit investors by allowing them to make more informed decisions. Similarly, other market participants that rely on financial statement information to provide services to investors would also benefit, because more informative and timely disclosure would allow them to better understand a registrant's cybersecurity risks and ability to manage such risks. As a result, they would be able to better evaluate registrants' securities and provide better recommendations.

[134] *See* Chris Florakis, Christodoulos Louca, Roni Michaely, and Michael Weber, *Cybersecurity Risk.* (No. w28196), Nat'l Bureau of Econ. Rsch, (2020).

[135] *See* Joshua Mitts and Eric Talley, *Informed Trading and Cybersecurity Breaches,* 9 Harv. Bus. L. Rev. 1 (2019) (''In many respects, then, the cyberhacker plays a role in creating and imposing a unique harm on the targeted company—one that (in our view) is qualitatively different from ''exogenous'' information shocks serendipitously observed by an information trader. Allowing a coordinated hacker-trader team to capture these arbitrage gains would implicitly subsidize the very harm-creating activity that is being ''discovered'' in the first instance.'').

[136] *Id.*

However, we note that the potential benefit could be reduced to the extent that registrants have already been providing the relevant disclosures.

We are unable to quantify the potential benefit to investors and other market participants as a result of the increase in disclosure and improvement in pricing under the proposed amendments. The estimation requires information about the fundamental value of securities and the extent of the mispricing. We do not have access to such information, and therefore cannot provide a reasonable estimate.

(ii) Greater Uniformity and Comparability

The proposed disclosure about cybersecurity incidents and cybersecurity risk management, strategy, and governance could also lead to more uniform and comparable disclosures, benefiting investors by lowering their search costs and information processing costs. As discussed in Section I, while some registrants currently file Form 8–K to report an incident, their reporting practices vary widely.[137] Some provide a discussion of materiality, the estimated costs of an incident, or the remedial steps taken as a result of an incident, while others do not provide such disclosure or provide much less detail in their disclosure. Disclosures related to risk management, strategy, and governance also vary significantly across registrants—such information could be disclosed in places such as the risk factors section, or in the management's discussion and analysis section of Form 10–K, or not at all. Investors currently may find it costly to compare the disclosures of different companies because they would have to spend time to search and retrieve information from different locations. For both types of disclosures, the proposed amendments would specify the topics to be disclosed and the reporting sections to include such disclosures, and as a result, both the incident disclosure and risk management, strategy, and governance disclosure should be more uniform across registrants, making it easier to compare. By specifying a set of topics that registrants should disclose, the proposed disclosure requirement should provide investors and other market participants with a benchmark of a minimum set of information for registrants to disclose, allowing them to better evaluate and compare registrants' cybersecurity risk and disclosure.

We note that to the extent that the disclosures related to cybersecurity risk management, strategy, and governance become too uniform or ''boilerplate,'' the benefit of comparability may be diminished. However, we also note that given the level of the specificity that would be required, the resulting disclosures are unlikely to become boilerplate.

The proposed requirement to tag the cybersecurity disclosure in Inline XBRL would likely augment the aforementioned informational and comparability benefits by making the proposed disclosures more easily retrievable and usable for aggregation, comparison, filtering, and other analysis. XBRL requirements for public operating company financial statement disclosures have been observed to mitigate information asymmetry by reducing information processing costs, thereby making the disclosures easier to access and analyze.[138]

While these observations are specific to operating company financial statement disclosures and not to disclosures outside the financial statements, such as the proposed cybersecurity disclosures, they suggest that the proposed Inline XBRL requirements could directly or indirectly (*i.e.,* through information intermediaries such as financial media, data aggregators, and academic researchers) provide investors with increased insight into cybersecurity-related information at specific companies and across companies, industries, and time periods.[139] Also,

[137] *See supra* section I.B.

[138] *See, e.g.,* J.Z. Chen, H.A. Hong, J.B. Kim, and J.W. Ryou, *Information processing costs and corporate tax avoidance: Evidence from the SEC's XBRL mandate,* 40 J. of Acct. and Pub. Pol'y. 2 (finding XBRL reporting decreases likelihood of firm tax avoidance because ''XBRL reporting reduces the cost of IRS monitoring in terms of information processing, which dampens managerial incentives to engage in tax avoidance behavior''); *see also* P.A. Griffin, H.A., Hong, J–B, Kim, and Jee-Hae Lim, *The SEC's XBRL Mandate and Credit Risk: Evidence on a Link between Credit Default Swap Pricing and XBRL Disclosure,* 2014 American Accounting Association Annual Meeting (2014) (finding XBRL reporting enables better outside monitoring of firms by creditors, leading to a reduction in firm default risk); *see also* E. Blankespoor, *The Impact of Information Processing Costs on Firm Disclosure Choice: Evidence from the XBRL Mandate,* 57 J. of Acc. Res. 919, 919–967 (2019) (finding ''firms increase their quantitative footnote disclosures upon implementation of XBRL detailed tagging requirements designed to reduce information users' processing costs,'' and ''both regulatory and non-regulatory market participants play a role in monitoring firm disclosures,'' suggesting ''that the processing costs of market participants can be significant enough to impact firms' disclosure decisions'').

[139] *See, e.g.,* N. Trentmann, *Companies Adjust Earnings for Covid–19 Costs, but Are They Still a One-Time Expense?,* The Wall Street J. (2020) (citing an XBRL research software provider as a source for the analysis described in the article); *see also Bloomberg Lists BSE XBRL Data,* XBRL.org (2018); *see also* R. Hoitash, and U. Hoitash,

unlike XBRL financial statements (including footnotes), which consist of tagged quantitative and narrative disclosures, the proposed cybersecurity disclosures would consist largely of tagged narrative disclosures.[140] Tagging narrative disclosures can facilitate analytical benefits such as automatic comparison or redlining of these disclosures against prior periods and the performance of targeted artificial intelligence or machine learning assessments (tonality, sentiment, risk words, etc.) of specific cybersecurity disclosures rather than the entire unstructured document.[141]

b. Benefits to Registrants [142]

The proposed amendments regarding both incident reporting and risk management, strategy, and governance disclosure could potentially lower registrants' cost of capital, especially for those who currently have strong cybersecurity risk management, strategy, and governance measures in place. Economic theory suggests that better disclosure could reduce information asymmetry between management and investors, reducing the cost of capital, and thereby improving firms' liquidity and their access to capital markets.[143] In an asymmetric information environment, investors recognize that registrants may take advantage of their position by issuing securities at a price that is higher than justified by the issuer's fundamental value. As a result, investors demand a discount to compensate for the risk of adverse selection. This discount translates into a higher cost of capital.[144] By providing more disclosure, the firm can reduce the risk of adverse selection faced by investors and the discount they demand, ultimately decreasing the firm's cost of capital.[145] Applying this theory to cybersecurity disclosure, the increased disclosure as a result of the proposed amendments could decrease the cost of capital and increase firm value.

The proposed amendments' effect on cost of capital might vary depending on registrants' current level of cybersecurity risk management, strategy, and governance and whether they are already making disclosures regarding their efforts. To the extent that they have not been making the proposed disclosure, registrants with stronger cybersecurity risk management, strategy, and governance measures could be priced more favorably under the proposed amendments because the proposed disclosure would allow the market to better differentiate them from the registrants with less robust measures. To the extent that some registrants are already making disclosures about their robust cybersecurity risk management, strategy, and governance programs, these registrants would benefit less. However, if registrants that previously had less robust cybersecurity risk management, strategy, and governance disclose improvements in their cybersecurity risk management, strategy, and governance in response to the proposed amendments, their cost of capital could also decrease.

Registrants could also benefit from more uniform regulations regarding the timing of disclosures and the types of cybersecurity incident and risk disclosures as a result of the proposed amendments. Currently, the stigma or reputation loss associated with cybersecurity breaches may result in companies limiting reporting about or delaying reporting of cybersecurity incidents.[146] If all registrants are required to report cybersecurity incidents on Form 8–K within four business days as proposed, this could reduce the reputation costs that any one company might suffer after reporting an attack and also reduce the incentives to underreport.

In addition, by formalizing the disclosure requirements related to cybersecurity incidents and cybersecurity risk management, strategy, and governance and specifying the topics to be discussed, the proposed amendments could reduce compliance costs for those registrants who are currently providing disclosure about these topics. The compliance costs would only be reduced to the extent that those registrants may be over-disclosing information, because there is uncertainty about what is required under the current rules. For instance,

Measuring Accounting Reporting Complexity with XBRL, 93 Account. Rev. 259 (2018).

[140] The proposed cybersecurity disclosure requirements do not expressly require the disclosure of any quantitative values; if a registrant includes any quantitative values that are nested within the required discussion (*e.g.,* disclosing the number of days until containment of a cybersecurity incident), those values would be individually detail tagged, in addition to the block text tagging of the narrative disclosures.

[141] To illustrate, without Inline XBRL, using the search term ''remediation'' to search through the text of all registrants' filings over a certain period of time, so as to analyze the trends in registrants' disclosures related to cybersecurity incident remediation efforts during that period, could return many narrative disclosures outside of the cybersecurity incident discussion (*e.g.,* disclosures related to potential environmental liabilities in the risk factors section). If Inline XBRL is used, however, it would enable a user to search for the term ''remediation'' exclusively within the proposed cybersecurity disclosures, thereby likely reducing the number of irrelevant results.

[142] While registrants are legally distinct entities from investors, benefits and costs to registrants as a result of the proposed amendments would ultimately accrue to their investors.

[143] *See* Douglas W. Diamond and Robert E. Verrecchia, *Disclosure, Liquidity, and the Cost of Capital,* 46 J. Fin. 1325, 1325–1359 (1991) (finding that revealing public information to reduce information asymmetry can reduce a firm's cost of capital through increased liquidity). *See also* Christian Leuz and Robert E. Verrecchia, *The Economic Consequences of Increased Disclosure,* 38 J. Acct. Res. 91 (2000) (providing empirical evidence that increased disclosure lowers the information asymmetry component of the cost of capital in a sample of German firms); *see also* Christian Leuz and Peter D. Wysocki, *The Economics of Disclosure and Financial Reporting Regulation: Evidence and Suggestions for Future Research,* 54 J. Acct. Res. 525 (2016) (providing a comprehensive survey of the literature on the economic effect of disclosure).

[144] *See* Leuz and Verrecchia, *The Economic Consequences of Increased Disclosure,* 38 J. Acct. Res. 91 (2000) (stating: ''A brief sketch of the economic theory is as follows. Information asymmetries create costs by introducing adverse selection into transactions between buyers and sellers of firm shares. In real institutional settings, adverse selection is typically manifest in reduced levels of liquidity for firm shares (*e.g.,* Copeland and Galai [1983], Kyle [1985], and Glosten and Milgrom [1985]). To overcome the reluctance of potential investors to hold firm shares in illiquid markets, firms must issue capital at a discount. Discounting results in fewer proceeds to the firm and hence higher costs of capital. A commitment to increased levels of disclosure reduces the possibility of information asymmetries arising either between the firm and its shareholders or among potential buyers and sellers of firm shares. This, in turn, should reduce the discount at which firm shares are sold, and hence lower the costs of issuing capital (*e.g.,* Diamond and Verrecchia [1991] and Baiman and Verrecchia [1996]).'').

[145] Although disclosure could be beneficial for the firm, several conditions must be met for firms to voluntarily disclose all their private information. *See* Anne Beyer, Daniel A. Cohen, Thomas Z. Lys, and Beverly R. Walther, *The Financial Reporting Environment: Review Of The Recent Literature,* 50 J. Acct. & Econ. 296, 296–343 (2010) (discussing conditions under which firms voluntarily disclose all their private information, and these conditions include ''(1) disclosures are costless; (2) investors know that firms have, in fact, private information; (3) all investors interpret the firms' disclosure in the same way and firms know how investors will interpret that disclosure; (4) managers want to maximize their firms' share prices; (5) firms can credibly disclose their private information; and (6) firms cannot commit ex-ante to a specific disclosure policy.''). Increased reporting could also help determine the effect of investment on firm value. *See* Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Lei Zhou, *The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective,* 34 (5) J. Acct. & Pub. Policy 509, 509–519 (2015) (arguing that ''information sharing could reduce the tendency by firms to defer cybersecurity investments.'').

[146] *See supra* note 133, Kamiya, at 720 (Kamiya et al.) (2021), (stating ''we find that successful cyberattacks have potentially economically large reputation costs in that the shareholder wealth loss far exceeds the out-of-pocket costs from the attack''). *See also* Eli Amir, Shai Levi, and Tsafrir Livne, *Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets,* 23 (3) Review of Accounting Studies 1177–1206 (2018) (finding evidence that is consistent with managers withholding information on cyber-attacks, and particularly the information on the more severe attacks).

the staff has observed that some registrants provide Form 8–K filings even when they do not anticipate the incident will have a material adverse impact on their business operations, or financial results.[147]

We are unable to quantify these potential benefits to registrants as a result of the proposed amendments due to lack of data. For example, we are unable to observe the actual cybersecurity risk registrants are facing. Without such information, we cannot provide a reasonable estimate on how registrants' cybersecurity risk and therefore their cost of capital may decrease.

2. Costs

We also recognize that enhanced cybersecurity disclosure could result in costs to registrants, depending on the timing and extent of the disclosure. These costs include potential increases in registrants' vulnerability, information uncertainty, and compliance costs. We discuss these costs below.

First, the proposed disclosure about cybersecurity incidents and cybersecurity risk management, strategy, and governance could potentially increase the vulnerability of registrants. Ever since the issuance of the 2011 Staff Guidance, concerns have been raised that providing detailed disclosures of cybersecurity incidents can create the risk of providing a road map for future attacks.[148] The concern is that malicious actors could use the disclosures to potentially gain insights into a registrant's practices on cybersecurity issues and thus better calibrate future attacks.

The proposed changes to Form 8–K and Form 6–K would require registrants to timely file current reports on these forms to disclose material cybersecurity incidents. The proposed disclosures include, for example, the nature and scope of the disclosed incident and whether the registrant has remediated or is currently remediating the incidents. While we have clarified that we would not expect a registrant to publicly disclose specific, 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 (to the extent that a registrant discloses information that could provide clues to malicious actors regarding a registrant's areas of vulnerability) it may face increased risk. Malicious actors could engage in further attacks based on the information, especially given that registrants would also need to make timely disclosure, which could mean that the underlying security issues might not have been completely resolved, thereby potentially exacerbating the ongoing attack. As a result, the proposed incident disclosure rules could potentially increase the vulnerability of registrants, imposing a cost on them and their investors.

Similar concerns could be raised about the proposed risk management, strategy, and governance disclosure. Specifically, proposed Item 407(j) would require registrants to disclose whether a member of its board of directors has cybersecurity expertise, and proposed new Items 106(b) and (c) would require registrants to provide specified disclosure regarding their cybersecurity policies and procedures and cybersecurity governance by a company's management and board. The required disclosure could provide malicious actors information about which companies lack a board of directors with cybersecurity expertise, and which ones have weak policies and procedures related to cybersecurity risk management, and allow such malicious actors to determine their targets accordingly.

However, academic research so far has not provided evidence that more detailed cybersecurity risk disclosures would necessarily lead to more attacks.[149] For example, one study finds that measures for specificity (*e.g.,* the uniqueness of the disclosure) do not have a statistically significant relation with subsequent cybersecurity incidents.[150] Another study finds that the disclosed security risk factors with risk-mitigation themes are less likely to be related to future breach announcements.[151] On the other hand, we note that the proposed amendments would require more details than under the current rules, and the uniformity of the proposed requirements might also make it easier for malicious actors to identify firms with deficiencies. Therefore, these findings might not be generalizable to the effects of the proposed amendments. Additionally, the costs resulting from this potential vulnerability might be partially mitigated to the extent that registrants may decide to enhance their cybersecurity risk management in anticipation of the increased disclosure.

Second, the proposed cybersecurity incident disclosure could potentially increase information uncertainty related to securities, because the disclosure about the impact of the incident on the registrant's operations may lack the precision needed for investors and the market to properly value these securities. While the proposed changes to Form 8–K could improve the timeliness of cybersecurity incident reporting and result in more disclosure about the impact of the incident on the registrant's operations, the proposed rules do not require registrants to quantify the impact of the incident. As a result, registrants' disclosure about the impact of a cybersecurity incident could be qualitative in nature or lack the precision needed for investors and the market to properly value the securities, potentially leading to information uncertainty, investor under or overreaction to certain disclosures, and thereby mispricing of registrants' securities.[152]

Additionally, while the proposed disclosure could have the overall effect of reducing registrants' cost of capital as discussed in Section III.C.1.b, we also recognize that a subset of registrants might experience an increase in costs of capital. More specifically, under the

[147] *See supra* note 129 and accompanying text.

[148] *See, e.g.,* Roland L. Trope and Sarah Jane Hughes, *The SEC Staff's Cybersecurity Disclosure Guidance: Will It Help Investors or Cyber-Thieves More,* 2011 Bus. L. Today 2, 1–4 (2011).

[149] We note that the papers we cited below study the effect of voluntary disclosure and 2011 Staff Guidance. The results from these studies might not be generalizable to the mandatory disclosures under the proposed rules.

[150] *See* He Li, Won Gyun No, and Tawei Wang, *SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors,* 30 Int'l. J. of Acct. Info. Sys. 40–55 (2018) (stating: ''while Ferraro (2013) criticizes that the SEC did little to resolve the concern about publicly revealing too much information [that] could provide potential hackers with a roadmap for successful attacks, we find no evidence supporting such claim'').

[151] *See* Tawei Wang, Karthik N. Kannan, and Jackie Rees Ulmer, *The Association Between the Disclosure and the Realization of Information Security Risk Factors,* 24.2 Info. Sys. Rsch. 201, 201–218 (2013).

[152] *See* Daniel Kent, David Hirshleifer, and Avanidhar Subrahmanyam, *Investor Psychology and Security Market under-and Overreactions,* J. of Fin. 1839–1885 (1998) (showing that investor behavioral biases such as overconfidence can cause them to under- or over-react to information); *see* Nicholas Barberis, Andrei Shleifer, and Robert Vishny, *A Model of Investor Sentiment,* 49 (3) J. of Fin. Econ. 307–343 (1998) (presenting a model of investor sentiment to explain the empirical findings of underreaction of stock prices to news such as earnings announcements, and overreaction of stock prices to a series of good or bad news based on two psychological phenomena, conservatism and representativeness heuristic); *see also* David Hirshleifer, *Investor Psychology and Asset Pricing,* 56 J. of Fin. 1533, 1533–1596 (2001) (stating: ''[m]ore generally, greater uncertainty about a set of stocks, and a lack of accurate feedback about their fundamentals, leaves more room for psychological biases. At the extreme, it is relatively hard to misperceive an asset that is nearly risk-free. Thus, the misvaluation effects of almost any mistaken-beliefs model should be strongest among firms about which there is high uncertainty/poor information (cash flow variance is one possible proxy).'').

proposed amendments, registrants with less robust cybersecurity risk management measures might be priced more unfavorably compared to those with stronger measures, potentially leading to an increase in cost of capital for these registrants. This is because the increased transparency as a result of the proposed disclosure could allow investors to better differentiate registrants' preparedness and ability to manage cybersecurity risks. However, except for this scenario, we expect that registrants overall would benefit from reduced cost of capital as a result of the proposed disclosure as discussed in Section III.C.1.b.

Finally, the proposed rules would impose compliance costs for registrants. Registrants would incur one-time and ongoing costs to fulfill the proposed new disclosure requirements under Items 106 and 407 of Regulation S–K. These costs would include costs to gather the information and prepare the disclosures.

Registrants would also incur compliance costs to fulfill the proposed disclosure requirements related to Form 8–K (Form 6–K for FPIs) incident reporting and Form 10–Q/10–K (Form 20–F for FPIs) ongoing reporting.[153] These costs include one-time costs to implement or revise their incident disclosure practices, so that any registrant that determines it has experienced a material cybersecurity incident would disclose such incident with the required information within four business days. Registrants would also incur ongoing costs to disclose in a periodic report any material changes, additions, or updates relating to previously disclosed incidents, and to monitor whether any previously undisclosed immaterial cybersecurity incidents have become material in the aggregate, triggering a disclosure obligation. The costs would be mitigated for registrants whose current disclosure practices match or are similar to those that are proposed. To the extent that registrants fall under other incident reporting requirements or cybersecurity risk management, strategy, and governance mandates as outlined in Section III.B.1, their costs from the proposed amendments would be mitigated as well.

We note that BDCs could be subject to both the proposed rules and rule amendments in the Investment Management Cybersecurity Proposing Release [154] and those proposed in this release if both proposals were to be adopted. To the extent that BDCs would need to provide substantively the same or similar disclosure on both Form 8–K and in registration statements, the compliance costs could be duplicative. However, the potential duplication should not result in a significant increase in compliance costs, because BDCs should be able to provide similar disclosure for both sets of rules.[155]

The compliance costs would also include costs attributable to the Inline XBRL tagging requirements. Various preparation solutions have been developed and used by operating companies to fulfill XBRL requirements, and some evidence suggests that, for smaller companies, XBRL compliance costs have decreased over time.[156] The incremental compliance costs associated with Inline XBRL tagging of cybersecurity disclosures would also be mitigated by the fact that most registrants who would be subject to the proposed requirements are already subject to other Inline XBRL requirements for other disclosures in Commission filings, including financial statement and cover page disclosures in certain periodic reports and registration statements.[157] Such registrants may be able to leverage existing Inline XBRL preparation processes and expertise in complying with the proposed cybersecurity disclosure tagging requirements. Asset-backed securities issuers, however, are not subject to Inline XBRL requirements in Commission filings and would likely incur initial Inline XBRL compliance implementation costs (such as the cost of training in-house staff to prepare filings in Inline XBRL, and the cost to license Inline XBRL filing preparation software from vendors).[158]

Other than the Paperwork Reduction Act costs discussed in Section IV below, we are unable to quantify the potential increase in costs related to the proposed rules due to the lack of data. For example, we lack data to estimate how registrants' cybersecurity vulnerability would change under the proposal, because such change would depend on their current level of vulnerability. We are also unable to estimate the potential increase in mispricing as a result of the information uncertainty, because the level of the uncertainty would depend on registrants' disclosure.

3. Indirect Economic Effects

Besides the direct economic effects on investors, registrants and other market participants we discussed above, we recognize that the proposed amendments could also indirectly affect registrants and external stakeholders, such as consumers, companies in the same industry with registrants or those facing similar cybersecurity threats.

While the proposal would only require disclosures—not changes to registrants' board composition or risk management practices—the disclosures themselves could result in certain indirect benefits. Registrants might respond to the proposed disclosures by devoting more resources to cybersecurity governance and risk management. To the extent that registrants may decide to enhance their cybersecurity risk management in anticipation of the increased disclosure, it could reduce registrants' susceptibility to a cybersecurity-attack and thereby the likelihood of future incidents, indirectly benefiting registrants.

Registrants may also decide to incur certain indirect costs as a result of the proposed amendments. For example, the proposed rules would require disclosure of whether members of the board or management staff have expertise in cybersecurity.

[153] We note that the compliance costs related to Form 6–K filings would be mitigated, because a condition of the form is that the information is disclosed or required to be disclosed elsewhere.

[154] *See* Investment Management Cybersecurity Proposing Release.

[155] *See infra* section VI.E.

[156] An AICPA survey of 1,032 reporting companies with $75 million or less in market capitalization in 2018 found an average cost of $5,850 per year, a median cost of $2,500 per year, and a maximum cost of $51,500 per year for fully outsourced XBRL creation and filing, representing a 45% decline in average cost and a 69% decline in median cost since 2014. *See* Michael Cohn, *AICPA Sees 45% Drop in XBRL Costs for Small Companies,* Accounting Today (Aug. 15, 2018) (stating that a 2018 NASDAQ survey of 151 listed registrants found an average XBRL compliance cost of $20,000 per quarter, a median XBRL compliance cost of $7,500 per quarter, and a maximum, XBRL compliance cost of $350,000 per quarter in XBRL costs per quarter), *available at https://www.accountingtoday.com/news/aicpa-sees-45-drop-in-xbrl-costs-for-small-reporting-companies* (retrieved from Factiva database); Letter from Nasdaq, Inc. (March 21, 2019) (to the Request for Comment on Earnings Releases and Quarterly Reports); *see* Release No. 33–10588 (Dec. 18, 2018) [83 FR 65601 (Dec. 21, 2018)].

[157] *See* 17 CFR 229.601(b)(101) and 17 CFR 232.405 (for requirements related to tagging financial statements, including footnotes and schedules in Inline XBRL). *See* 17 CFR 229.601(b)(104) and 17 CFR 232.406 (for requirements related to tagging cover page disclosures in Inline XBRL).

[158] *See infra* section IV.

Although not required, some registrants may respond by adding a board member or staff to their management team with cybersecurity expertise. Similarly, the proposed rules would require disclosure on policies and procedures to identify and manage cybersecurity risks. While not required under the proposed rules, it is possible that registrants would respond by allocating more resources to devise, implement, or improve their policies and procedures related to cybersecurity to the extent they currently do not have similar policies and procedures in place. Similarly, indirect costs could result if a registrant were to decide to hire a chief information security officer or other individuals with cybersecurity expertise to their management team. Further, if many registrants move to add a board member or staff to their management team with cybersecurity expertise, or a chief information security officer at the same time, the costs to registrants associated with adding such individuals may increase if demand for cybersecurity expertise increases. This is especially true to the extent that certain relevant certifications or degrees are seen as important designations of cybersecurity expertise and there are a limited pool of individuals holding such certifications.

In addition, the proposed requirement to tag the cybersecurity disclosure in Inline XBRL could have indirect effects on registrants. As discussed in section III.C.1.a.(ii), XBRL requirements for public operating company financial statement disclosures could reduce information processing cost. This reduction in information processing cost has been observed to facilitate the monitoring of companies by other market participants, and, as a result, to influence companies' behavior, including their disclosure choices.[159]

The proposed amendments to require registrants to timely disclose material cybersecurity incidents could indirectly benefit external stakeholders such as other companies in the same industry, those facing similar cybersecurity threats or consumers. Cybersecurity incidents could result in costs not only to the company that suffers the incident, but also to other businesses and consumers. For example, a cybersecurity breach at one company may cause a major disruption or shut down of a critical infrastructure industry, such as a gas pipeline, a bank, or power company, resulting in massive losses throughout the economy.[160] Timely disclosure of cybersecurity incidents as proposed could increase awareness by those external stakeholders that the malicious activities are occurring. More specifically, for companies in the same industry as registrants or for those facing similar cybersecurity threats, the proposed disclosure could alert them to a potential threat and allow them to better prepare for a specific potential cybersecurity attack. To the extent that the proposed amendments increase available disclosure, consumers may benefit from learning the extent of a particular cybersecurity breach, and therefore take appropriate actions to limit potential economic costs that they may incur from the breach. For example, there is evidence that increased disclosure of cybersecurity incidents by registrants can reduce the risk of identity theft for individuals.[161] Also, consumers may be able to make better informed decisions about which companies to trust with their personal information.

In addition, the proposed amendments regarding cybersecurity risk management, strategy, and governance disclosure could indirectly benefit external stakeholders through potentially reduced likelihood of future incidents and negative externalities associated with the incidents. As discussed above, to the extent that registrants may decide to enhance their cybersecurity risk management in anticipation of the increased disclosure, it could reduce registrants' susceptibility to a cybersecurity-attack and thereby the likelihood of future incidents, leading to positive spillover effects.

We are unable to quantify the indirect effects as a result of the proposed amendments because we lack data or basis to estimate the potential changes in disclosure of cybersecurity incidents, risk management, strategy, and governance disclosure and the reduction in negative spill-over effects.

D. Anticipated Effects on Efficiency, Competition, and Capital Formation

Overall, we believe the proposed rules could have positive effects on market efficiency. As discussed above, the proposed rules could improve the timeliness and informativeness of cybersecurity risk disclosure. Investors and other market participants could better understand the cybersecurity threats registrants are facing, their potential impact, and registrants' ability to respond to and manage risks under the proposed rules, and thereby better evaluate registrants' securities and make more informed decisions. As a result, the proposed disclosures could reduce information asymmetry and mispricing in the market, improving liquidity and market efficiency. However, we also recognize that, because registrants' disclosure about the impact of a cybersecurity incident could be qualitative in nature and lack the precision needed for investors and the market to properly value the securities, the proposed incident disclosure might lead to information uncertainty and investor overreaction. We believe such effect should be reduced by more informative reporting from other aspects of the proposed disclosure and subsequent updates in periodic reports.

A more efficient market as a result of the proposed rules could promote competition among firms. Because the enhanced incident reporting and cybersecurity risk management, strategy, and governance disclosure could allow investors to better evaluate the relative cybersecurity risks for different registrants, firms that disclose robust cybersecurity risk management, strategy, and governance could benefit from a competitive advantage relative to firms that do not. This could have a secondary effect of further incentivizing firms that to-date have invested less in cybersecurity preparation to invest more, to the benefit of investors, in order to become more competitive.

[159] *See supra* note 138.

[160] *See* Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Lei Zhou, *Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model,* 6 (1) J. of Info. Sec. 24, 24–30 (2014) (stating: ''[f]irms in the private sector of many countries own a large share of critical infrastructure assets. Hence, cybersecurity breaches in private sector firms could cause a major disruption of a critical infrastructure industry (*e.g.,* delivery of electricity), resulting in massive losses throughout the economy, putting the defense of the nation at risk.''). We note that this study focused on private firms; however, same statement could be made about public companies that own a large share of critical infrastructure assets. *See also U.S. Pipeline Cyberattack Forces Closure,* Wall St J., *available at https://www.wsj.com/articles/cyberattack-forces-closure-of-largest-u-s-refined-fuel-pipeline-11620479737.*

[161] *See* Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft*?, 30 (2) J. of Pol'y. Analysis and Mgmt. 272, 256–286 (2011) (finding that the adoption of state-level data breach disclosure laws reduced identity theft by 6.1 percent).

More efficient prices and more liquid markets could help allocate capital to its most efficient uses. Enhanced disclosure of cybersecurity incidents and cybersecurity risk management, strategy, and governance could allow investors to make more informed investment decisions. As a result, companies that disclose more robust cybersecurity risk management, strategy, and governance and thus may be less susceptible to cybersecurity incidents may receive more capital allocation. By making information related to material incident available to the public sooner, and reducing the information asymmetry, the proposed amendments could increase public trust in markets, thereby aiding in capital formation.

D. Reasonable Alternatives

1. Website Disclosure

As an alternative to Form 8–K disclosure of material cybersecurity incidents, we considered providing companies with the option of disclosing this information through company websites, instead of through filing a Form 8–K, when the company has disclosed its intention to do so in its most recent annual report and subject to information availability and retention requirements. While this approach may be less costly for the registrant as it may involve fewer compliance costs and less legal liability compared to a filing of a Form 8–K, the website disclosure would not be located in the same place as other companies' disclosures of material cybersecurity incidents. Also, disclosures made on company websites would not be organized into the standardized sections found in Form 8–K and could thus be less uniform.

The lack of a central repository, such as the EDGAR system,[162] and a lack of uniformity of website disclosures could increase the costs for investors and other market participants to search for and process the information to compare cybersecurity risks across registrants. Additionally, such disclosure might not be preserved on the company's website for as long as it would be when the disclosure is filed with the Commission, because companies may not keep historical information available on their websites indefinitely. They also may go out of business, and thus, there could be information loss to investors when disclosures are deleted from websites. Therefore, this approach would be less beneficial to investors, other market participants, and the overall efficiency of the market.

2. Disclosure Through Form 10–Q and Form 10–K

We also considered requiring disclosure of material cybersecurity incidents through Form 10–Q or Form 10–K instead of Form 8–K. Reporting material cybersecurity incidents at the end of the quarter or year would allow registrants more time to assess the financial impact of such incidents. The resulting disclosure might be more specific or informative for investors and other market participants to value the securities and make more informed decisions. The compliance costs would be less under this alternative, because registrants would not have an obligation to file Form 8–K. With lower compliance costs under this alternative, registrants could use the resources that would go towards disclosure on Form 8–K to instead fill gaps in their cybersecurity defenses exposed by the attack, potentially making it less likely that malicious actors would be able to exploit such vulnerabilities.

However, it would lead to less timely reporting on material cybersecurity incidents. As a result, the market would not be able to incorporate the information related to cybersecurity risk into the security prices in as timely a manner, and investors and other market participants would not be able to make as informed decisions as they could under the proposed approach.

3. Exempt Smaller Reporting Companies

We also considered exempting smaller reporting companies from proposed Item 106 and Item 407, because smaller companies might incur a cost that is disproportionally high, compared to larger companies under the proposed rules. As discussed above, proposed disclosure might expose registrants' cybersecurity weakness and increase their vulnerability. To avoid the potential exposure, smaller companies might increase spending related to cybersecurity risk management measures, which could be disproportionately costly. Also, to the extent that they do not have similar disclosure practices in place currently, it might be relatively more costly for smaller companies to implement the proposed disclosure requirements than larger companies, because they may have fewer resources.

However, evidence suggests that smaller companies may have an equal or greater risk than larger companies of being attacked, making the proposed disclosures particularly important for their investors.[163] The financial impact from an attack could also be more detrimental for smaller companies than for larger ones. To the extent that one indirect effect of the proposed disclosure may be that companies take additional steps to address potential vulnerabilities or enhance their cybersecurity risk management, strategy, and governance, any resulting reduction in vulnerability may be particularly beneficial for smaller companies and their investors.

4. Modify Scope of Inline XBRL Requirement

We also considered changing the scope of the proposed tagging requirements, such as by excluding certain subsets of registrants. For example, the proposed tagging requirements could have excluded asset-backed securities issuers, which are not currently required to tag any filings in Inline XBRL.[164] Under such an alternative, asset-backed securities issuers would submit their cybersecurity disclosures in unstructured HTML or ASCII, and thereby avoid the initial Inline XBRL implementation costs (such as the cost of training in-house staff to prepare filings in Inline XBRL, and the cost to license Inline XBRL filing preparation software from vendors) and ongoing Inline XBRL compliance burdens that would result from the proposed tagging requirement.[165] However, narrowing the scope of the proposed tagging requirements, whether based on registrant type, size, or other criteria, would diminish the extent of any informational benefits that would accrue as a result of the proposed disclosure requirements by making the excluded registrants' cybersecurity disclosures comparatively costlier to process and analyze.

[162] EDGAR, the Electronic Data Gathering, Analysis, and Retrieval system, is the primary system for companies and others submitting documents under the Securities Act, the Exchange Act, the Trust Indenture Act of 1939, and the Investment Company Act. EDGAR's public database can be used to research a public company's financial information and operations.

[163] *See supra* note 18.

[164] *See supra* note 157.

[165] *See infra* section IV. The Commission's EDGAR electronic filing system generally requires filers to use ASCII or HTML for their document submissions, subject to certain exceptions. *See* EDGAR Filer Manual (Volume II) version 60 (December 2021), at 5–1; 17 CFR 232.301 (incorporating EDGAR Filer Manual into Regulation S–T). *See also* 17 CFR 232.101 (setting forth the obligation to file electronically on EDGAR). To the extent asset-backed securities issuers are affiliated with registrants that are subject to Inline XBRL requirements, they may be able to leverage those registrants' existing Inline XBRL tagging experience and software, which would mitigate the initial Inline XBRL implementation costs that asset-backed securities issuers would incur under the proposal.

Request for Comment

We request comment on all aspects of our economic analysis, including the potential costs and benefits of the proposed rules and alternatives thereto, and whether the proposed rules, if adopted, would promote efficiency, competition, and capital formation or have an impact on investor protection. In addition, we also seek comment on alternative approaches to the proposed rules and the associated costs and benefits of these approaches. Commenters are requested to provide empirical data, estimation methodologies, and other factual support for their views, in particular, on costs and benefits estimates. Specifically, we seek comment with respect to the following questions:

41. What are the economic effects of the proposed cybersecurity incident and cybersecurity risk management, strategy, and governance disclosures? Would those disclosures provide informational benefits to investors? Would registrants benefit from a potential decrease in cost of capital because of the enhanced disclosure? Are there any other benefits, costs, and indirect effects of the proposed disclosure that we should also consider?

42. Would the proposed cybersecurity incident disclosure provide enough information for investors to assess the impact of a cybersecurity incident in making an investment decision? Because the proposed incident disclosure would not require quantification of an incident's impact, would the lack of quantification create any uncertainty for investors which may cause them to under or overreact to the disclosure? Would investors benefit more if registrants were to provide the disclosure after the incident's impact is quantified or can be reasonably estimated? If so, what metrics should be disclose to help investors understand the impact?

43. Would both types of the proposed disclosure, cybersecurity incident disclosure and cybersecurity risk management, strategy, and governance disclosure, increase the vulnerability of registrants to cybersecurity incidents? Would this effect be mitigated by any of the other effects of the proposal, including indirect effects such as registrants' potential strengthening of cybersecurity risk management measures? What would be the impact of the proposed disclosure on the likelihood of future incidents for registrants? Would that impact be the same for both types of disclosure?

44. Would the proposed incident disclosure increase registrants' compliance costs to fulfill the proposed disclosure requirements related to incident reporting? What would be the magnitude of those costs? Would the proposed cybersecurity risk management, strategy, and governance disclosure lead to indirect costs such as hiring a board member or staff to their management team with cybersecurity expertise, or costs to devise, implement or improve the processes and procedures related to cybersecurity?

45. Would both types of the proposed disclosure lead to indirect economic effects for external stakeholders? Would the magnitude of the indirect effects be greater or less than we have discussed? Are there any other indirect effects that we should consider?

46. Are there any specific data points that would be valuable for assessing the economic effects of the proposed cybersecurity incident and risk management, strategy, and governance that we should consider in the baseline analysis or the analysis of the economic effects? If so, please provide that data.

47. Would any of the economic effects discussed above be more or less significant than in our assessment? Are any of the costs or benefits identified incorrectly for any of the proposed amendments? Are there any other economic effects associated with these proposed rules that we should consider? Are you aware of any data or methodology that can help quantify the benefits or costs of the proposed amendments?

48. Would any of the proposed amendments positively affect efficiency, competition and capital formation as we have discussed? Are there any other effects on efficiency, competition, and capital formation that we should consider?

49. Would any of the proposed amendments have disproportionate costs for smaller reporting companies? Do smaller reporting companies face a different set of cybersecurity risks than other companies?

50. Are there any other alternative approaches to improve disclosure of material cybersecurity incidents, cybersecurity risk management, strategy, or governance that we should consider? If so, what are they and what would be the associated costs or benefits of these alternative approaches?

51. Are there any other costs and benefits associated with alternative approaches that are not identified or are misidentified in the above analysis? Should we consider any of the alternative approaches outlined above instead of the proposed rules? Which approach and why?

IV. Paperwork Reduction Act

A. Summary of the Collection of Information

Certain provisions of our rules and forms that would be affected by the proposed amendments contain ''collection of information'' requirements within the meaning of the Paperwork Reduction Act of 1995 (''PRA'').[166] The Commission is submitting the proposed amendments to the Office of Management and Budget (''OMB'') for review in accordance with the PRA.[167] The hours and costs associated with preparing and filing the forms constitute reporting and cost burdens imposed by each collection of information. An agency may not conduct or sponsor, and a person is not required to comply with, a collection of information unless it displays a currently valid OMB control number. Compliance with the information collections is mandatory. Responses to the information collections are not kept confidential and there is no mandatory retention period for the information disclosed. The titles for the affected collections of information are:

- ''Schedule 14C'' (OMB Control No. 3235–0057);
- ''Schedule 14A'' (OMB Control No. 3235–0059);
- ''Form 8–K'' (OMB Control No. 3235–0060);
- ''Form 10–K'' (OMB Control No. 3235–0063);
- ''Form 10–Q'' (OMB Control No. 3235–0070);
- ''Form 6–K'' (OMB Control No. 3235–0116); and
- ''Form 20–F'' (OMB Control No. 3235–0288).

We adopted the existing forms, pursuant to the Exchange Act. The forms set forth the disclosure requirements for periodic and current reports as well as proxy and information statements filed by issuers to help investors make informed investment and voting decisions. A description of the proposed amendments, including the need for the information and its proposed use, as well as a description of the likely respondents, can be found in Section II above, and a discussion of the economic effects of the proposed amendments can be found in Section III above.

[166] *See* 44 U.S.C. 3501 *et seq.*

[167] 44 U.S.C. 3507(d) and 5 CFR 1320.11.

B. Summary of the Estimated Burdens of the Proposed Amendments on the Collections of Information

Estimated Paperwork Burdens of the Proposed Amendments

The following table summarizes the estimated paperwork burdens associated with the proposed amendments to the affected forms.

PRA TABLE 1—ESTIMATED PAPERWORK BURDEN ASSOCIATED WITH THE PROPOSED NEW RULES AND AMENDMENTS *

Proposed requirements and effects	Affected forms and schedules	Estimated burden per response	Number of estimated affected responses
Form 8–K, Item 1.05:			
• Require disclosure regarding cybersecurity incidents.	Form 8–K	10 Hours	200 Filings.
Form 6–K:			
• Require disclosure regarding cybersecurity incidents.	Form 6–K	9 Hours	20 Filings.
Adding Item 106 Disclosures:			
• Require disclosure regarding policies and procedures. (Item 106(b)).	• Form 10–K	• Form 10–K: 15 Hours **	• Form 10–K: 8,292 Filings.
• Require disclosure regarding board and management oversight of cybersecurity risk. (Item 106(c)).	• Form 20–F	• Form 20–F: 16.5 Hours.	• Form 20–F: 729 Filings.
• Require updated disclosure regarding cybersecurity incidents (Item 106(d)).	• Form 10–Q (Item 106(d)).	• Form 10–Q: 5 Hours.	• Form 10–Q: 600 Filings.
Adding Item 407(j) disclosures:			
• Require disclosure on the cybersecurity expertise of members of the board of directors of the registrant, if any.	• Form 10–K • Schedule 14A • Schedule 14C.	• Form 10–K: 1.5 Hours • Schedule: 14A: 1.5 Hours. • Schedule 14C: 1.5 Hours ±.	• Form 10–K: Filings: 5,464 Filings. • Schedule 14A: 2,600 Filings. • Schedule 14C: 228 Filings.

* All of these burden estimates incorporate the proposed tagging requirements Rule 405 of Regulation S–T.
** We estimate that 600 of these filings will be increased by five hours due to the proposed Item 106(d) disclosure.
± The burden estimate for Form 10–K assumes that Schedules 14A and 14C would be the primary disclosure documents for the information provided in response to proposed Item 407(j) of Regulation S–K in connection with proxy and information statements involving the election of directors. In this case, we assume that the disclosure would be incorporated by reference in Form 10–K from the proxy or information statement.

Not every filing on the affected current forms, Form 6–K and Form 8–K, would include cybersecurity disclosures. These disclosures would be required only when a registrant has made the determination that it has experienced a material cybersecurity incident. Further, in the case of Form 6–K, the registrant would only have to provide the disclosure if it is required to disclose such information elsewhere.

The table below sets forth our estimates of the number of current filings on the forms which will be affected by the proposed rules. We used this data to extrapolate the effect of these changes on the paperwork burden for the listed periodic reports.[168]

PRA TABLE 3—ESTIMATED NUMBER OF AFFECTED FILINGS

Form	Current annual responses in PRA inventory	Estimated number of filings that would include cybersecurity disclosure
Schedule 14A	6,369	2,600
Schedule 14C	569	228
10–K	8,292	8,292
10–Q	22,925	600
20–F	729	729
8–K	118,387	200
6–K	34,794	20

C. Incremental and Aggregate Burden and Cost Estimates

Below we estimate the incremental and aggregate changes in paperwork burden as a result of the proposed amendments. These estimates represent the average burden for all respondents, both large and small. In deriving our estimates, we recognize that the burdens will likely vary among individual respondents based on a number of factors, including the nature of their business.

We calculated the additional burden estimates by multiplying the estimated additional burden per form by the estimated number of responses per form. That additional burden is then added to the existing burden per form. For purposes of the PRA, the burden is

[168] The OMB PRA filing inventories represent a three-year average. Averages may not align with the actual number of filings in any given year.

to be allocated between internal burden hours and outside professional costs. PRA Table 4 below sets forth the percentage estimates we typically use for the burden allocation for each collection of information and the estimated burden allocation for the proposed new collection of information. We also estimate that the average cost of retaining outside professionals is $400 per hour.[169]

PRA TABLE 4—ESTIMATED BURDEN ALLOCATION FOR THE AFFECTED COLLECTIONS OF INFORMATION

Collection of information	Internal (percent)	Outside professionals (percent)
Schedule 14A, Schedule 14C, Form 10–Q, Form 10–K, Form 6–K, and Form 8–K	75	25
Form 20–F	25	75

PRA Table 5 below illustrates the incremental change to the total annual compliance burden of affected forms, in hours and in costs, as a result of the proposed amendments' estimated effect on the paperwork burden per response.

PRA TABLE 5—CALCULATION OF THE INCREMENTAL CHANGE IN BURDEN ESTIMATES OF CURRENT RESPONSES RESULTING FROM THE PROPOSED AMENDMENTS

Collection of information	Number of estimated affected responses (A) [a]	Burden hour increase per response (B)	Change in burden hours (C) = (A) × (B)	Change in company hours (D) = (C) × 0.75 or .25	Change in professional hours (E) = (C) × 0.25 or .75	Change in professional costs (F) = (E) × $400
Schedule 14A	2,600	1.5	3,900	2,925	975	$390,000
Schedule 14C	228	1.5	342	256.50	85.50	34,200
10–K	8,292	15	124,380	93,285	31,095	12,438,000
10–K	5,464	1.5	8,196	6,147	2,049	819,600
10–Q	600	5	3,000	2,250	750	300,000
20–F	729	16.5	12,028.50	3,007.125	9,021.375	3,608,550
8–K	200	10	2,000	1,500	500	200,000
6–K	20	9	180	135	45	18,000

The following tables summarize the requested paperwork burden, including the estimated total reporting burdens and costs, under the proposed amendments.

PRA TABLE 6—REQUESTED PAPERWORK BURDEN UNDER THE PROPOSED AMENDMENTS *

Form	Current burden			Program change			Requested change in burden		
	Current annual responses (A)	Current burden hours (B)	Current cost burden (C)	Number of affected responses (D)	Change in company hours (E)	Change in professional costs (F)	Annual responses (G) = (A)	Burden hours (H) = (B) + (E)	Cost burden (I) = (C) + (F)
Schedule 14A	6,369	777,590	$103,678,712	2,600	2,925	$390,000	6,369	780,515	$104,068,712
Schedule 14C	569	56,356	7,514,944	228	256.50	34,200	569	56,613	7,529,144
Form 10–K	8,292	14,188,040	1,893,793,119	8,292 (Item 106). 5,464 (407(j))	99,432 93,285 (Item 106) 6,147 (407(j))	13,257,600 (12,438,000 + 819,600)	8,292	14,287,432	1,907,050,719
Form 10–Q	22,925	3,182,333	421,490,754	600	2,250	300,000	22,925	3,184,583	421,790,754
Form 20–F	729	479,261	576,824,025	729	3,007.125	3,608,550	729	482,268	580,432,575
Form 8–K	118,387	818,158	108,674,430	200	1,500	200,000	118,387	819,658	108,847,430
Form 6–K	34,794	227,031	30,270,780	20	135	18,000	34,794	227,166	30,288,780

* For purposes of the PRA, the requested change in burden hours (column H) is rounded to the nearest whole number.

Request for Comment

Pursuant to 44 U.S.C. 3506(c)(2)(B), we request comment in order to:

- Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility;
- Evaluate whether the Commission's estimates of the burden of the proposed collection of information are accurate;
- Determine whether there are ways to enhance the quality, utility, and

[169] We recognize that the costs of retaining outside professionals may vary depending on the nature of the professional services, but for purposes of this PRA analysis, we estimate that such costs would be an average of $400 per hour. This estimate is based on consultations with several issuers, law firms, and other persons who regularly assist issuers in preparing and filing reports with the Commission.

clarity of the information to be collected;

• Evaluate whether there are ways to minimize the burden of the collection of information on those who respond, including through the use of automated collection techniques or other forms of information technology; and

• Evaluate whether the proposed amendments would have any effects on any other collection of information not previously identified in this section.

Any member of the public may direct to us any comments concerning the accuracy of these burden estimates and any suggestions for reducing these burdens. Persons submitting comments on the collection of information requirements should direct their comments to the Office of Management and Budget, Attention: Desk Officer for the U.S. Securities and Exchange Commission, Office of Information and Regulatory Affairs, Washington, DC 20503, and send a copy to Vanessa A. Countryman, Secretary, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549, with reference to File No. S7–09–22 Requests for materials submitted to OMB by the Commission with regard to the collection of information requirements should be in writing, refer to File No. S7–09–22 and be submitted to the U.S. Securities and Exchange Commission, Office of FOIA Services, 100 F Street NE, Washington DC 20549. OMB is required to make a decision concerning the collection of information requirements between 30 and 60 days after publication of the proposed amendments. Consequently, a comment to OMB is best assured of having its full effect if the OMB receives it within 30 days of publication.

V. Small Business Regulatory Enforcement Fairness Act

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996 (''SBREFA''),[170] the Commission must advise OMB as to whether the proposed amendments constitute a ''major'' rule. Under SBREFA, a rule is considered ''major'' where, if adopted, it results or is likely to result in:

• An annual effect on the U.S. economy of $100 million or more (either in the form of an increase or a decrease);

• A major increase in costs or prices for consumers or individuals industries; or

• Significant adverse effects on competition, investment, or innovation.

We request comment on whether the proposed amendments would be a ''major rule'' for purposes of SBREFA. In particular, we request comment on the potential effect of the proposed amendments on the U.S. economy on an annual basis; any potential increase in costs or prices for consumers or individual industries; and any potential effect on competition, investment or innovation. Commenters are requested to provide empirical data and other factual support for their views to the extent possible.

VI. Initial Regulatory Flexibility Act Analysis

When an agency issues a rulemaking proposal, the Regulatory Flexibility Act (''RFA'') [171] requires the agency to prepare and make available for public comment an Initial Regulatory Flexibility Analysis (''IRFA'') that will describe the impact of the proposed rule on small entities.[172] This IRFA relates to proposed amendments and/or additions to the rules and forms described in Section II above.

A. Reasons for, and Objectives of, the Proposed Action

The proposed amendments are intended to provide enhanced disclosures regarding registrants' cybersecurity risk governance and cybersecurity incident reporting. They are designed to better inform investors about material cybersecurity risks and incidents on a timely basis and a registrant's assessment, governance, and management of those risks. The proposed amendments are discussed in more detail in Section II above. We discuss the economic impact and potential alternatives to the amendments in Section III, and the estimated compliance costs and burdens of the amendments under the PRA in Section IV above.

B. Legal Basis

The amendments contained in this release are being proposed under the authority set forth in Securities Act Sections 7 and 19(a) and Exchange Act Sections 3(b), 12, 13, 14, 15, and 23(a).

C. Small Entities Subject to the Proposed Rules

The proposed amendments would apply to registrants that are small entities. The Regulatory Flexibility Act defines ''small entity'' to mean ''small business,'' ''small organization,'' or ''small governmental jurisdiction.'' [173] For purposes of the Regulatory Flexibility Act, under our rules, a registrant, other than an investment company, is a ''small business'' or ''small organization'' if it had total assets of $5 million or less on the last day of its most recent fiscal year and is engaged or proposing to engage in an offering of securities that does not exceed $5 million.[174] Under 17 CFR 270.0–10, an investment company, including a BDC, is considered to be a small entity if it, together with other investment companies in the same group of related investment companies, has net assets of $50 million or less as of the end of its most recent fiscal year.[175] An investment company, including a BDC,[176] is considered to be a ''small business'' if it, together with other investment companies in the same group of related investment companies, has net assets of $50 million or less as of the end of its most recent fiscal year.[177] Commission staff estimates that, as of June 2021, there were 660 issuers,[178] and 9 BDCs [179] that may be considered small entities that would be subject to the proposed amendments.

D. Projected Reporting, Recordkeeping and Other Compliance Requirements

If adopted, the proposed amendments would apply to small entities to the same extent as other entities, irrespective of size. Therefore, we expect that the nature of any benefits and costs associated with the proposed amendments to be similar for large and small entities. Accordingly, we refer to the discussion of the proposed amendments' economic effects on all affected parties, including small entities, in Section III above. Consistent with that discussion, we anticipate that the economic benefits and costs likely could vary widely among small entities based on a number of factors, such as the nature and conduct of their businesses, which makes it difficult to project the economic impact on small entities with precision. As a general matter, however, we recognize that the costs of the proposed amendments borne by the affected entities could have a proportionally greater effect on small

[170] 5 U.S.C. 801 *et seq.*

[171] 5 U.S.C. 601 *et seq.*

[172] 5 U.S.C. 603(a).

[173] 5 U.S.C. 601(6).

[174] *See* 17 CFR 240.0–10(a).

[175] 17 CFR 270.0–10(a).

[176] BDCs are a category of closed-end investment company that are not registered under the Investment Company Act [15 U.S.C. 80a–2(a)(48) and 80a–53–64].

[177] 17 CFR 270.0–10(a).

[178] This estimate is based on staff analysis of Form 10–K filings on EDGAR, or amendments thereto, filed during the calendar year of Jan. 1, 2020 to Dec. 31, 2020, or filed by Sept. 1, 2021, and on data from XBRL filings, Compustat, and Ives Group Audit Analytics.

[179] These estimates are based on staff analysis of Morningstar data and data submitted by investment company registrants in forms filed on EDGAR as of June 30, 2021.

entities, as they may be less able to bear such costs relative to larger entities.

Compliance with the proposed amendments may require the use of professional skills, including legal skills. We request comment on how the proposed disclosure amendments would affect small entities.

E. Duplicative, Overlapping, or Conflicting Federal Rules

The Commission has also proposed cybersecurity risk management rules and related rule amendments for advisers and funds, including BDCs. To the extent that the proposed rules and rule amendments in the Investment Management Cybersecurity Proposing Release are adopted, BDCs may be subject both to those proposed rules and rule amendments and to certain of the rules proposed in this rulemaking. To the extent that there could be overlap if these proposals are adopted, we would not expect the overlap to result in significant burdens for BDCs (including small BDCs) since they should be able to use their Form 8–K disclosure to more efficiently prepare the corresponding disclosure that would be required by the Investment Management Cybersecurity Proposing Release or, in the alternative, use that corresponding disclosure (if adopted) to prepare their Form 8–K disclosure.

F. Significant Alternatives

The RFA directs us to consider alternatives that would accomplish our stated objectives, while minimizing any significant adverse impact on small entities. In connection with the proposed amendments, we considered the following alternatives:

- Establishing different compliance or reporting requirements that take into account the resources available to small entities;
- Exempting small entities from all or part of the requirements;
- Using performance rather than design standards; and
- Clarifying, consolidating, or simplifying compliance and reporting requirements under the rules for small entities.

The proposed amendments are intended to better inform investors about cybersecurity incidents and the cybersecurity risk management, strategy, and governance of registrants of all types and sizes which are subject to the Exchange Act reporting requirements. Under current requirements, the nature of registrants' cybersecurity disclosure varies widely, with registrants providing different levels of specificity regarding the cause, scope, impact and materiality of cybersecurity incidents. The timing of disclosure about material cybersecurity incidents also varies in the absence of a specific requirement regarding timely disclosure of such incidents. Further, while registrants generally discuss cybersecurity risks in the risk factor section of their annual reports, the disclosures are sometimes blended with other unrelated disclosures, which makes it more difficult for investors to locate, interpret, and analyze the information provided. The staff also has observed a divergence in these disclosures by industry and that smaller reporting companies generally provide less cybersecurity disclosure as compared to larger registrants.

Exempting small entities from the proposed amendments or establishing different compliance or reporting requirements for small entities could frustrate the goal of providing investors in these companies with more uniform and timely disclosure about material cybersecurity incidents and disclosure about their risk management and governance practices that is comparable to the disclosure provided by other registrants. Further, as stated in Sections II and III of this release, evidence suggests that smaller companies may have an equal or greater risk than larger companies of being attacked, making the proposed disclosures particularly important for investors in these companies.[180] Therefore, our objectives would not be served by establishing different compliance or reporting requirements for small entities or clarifying, consolidating or simplifying compliance and reporting requirements for small entities.

With respect to using performance rather than design standards, the proposed amendments use primarily use design rather than performance standards to promote more consistent and comparable disclosures by all registrants.

Section II of this release includes specific requests for comment on whether certain categories of registrants, including smaller reporting companies, should be exempted from the proposed Regulation S–K Item 106 disclosure regarding cybersecurity risk management, strategy and governance. The release also requests comment on how any exemption would impact investor assessments and comparisons of the cybersecurity risks of registrants. In addition, comment is solicited on whether smaller reporting companies should be exempted from the board expertise disclosure requirement in proposed Item 407(j) and from the requirements to present the proposed disclosure in Inline XBRL.

[180] *See supra* note 18. *See* Section III.E.3.

Request for Comment

We encourage the submission of comments with respect to any aspect of this IRFA. In particular, we request comments regarding:

- The number of small entities that may be affected by the proposed amendments;
- The existence or nature of the potential impact of the proposed amendments on small entities discussed in the analysis;
- How the proposed amendments could further lower the burden on small entities; and
- How to quantify the impact of the proposed amendments.

Commenters are asked to describe the nature of any impact and provide empirical data supporting the extent of the impact. Comments will be considered in the preparation of the Final Regulatory Flexibility Analysis, if the proposed amendments are adopted, and will be placed in the same public file as comments on the proposed amendments themselves.

Statutory Authority and Text of Proposed Rule and Form Amendments

We are proposing the rule and form amendments contained in this document under the authority set forth in Sections 7 and 19(a) of the Securities Act and Sections 3(b), 12, 13, 14, 15, and 23(a) of the Exchange Act.

List of Subjects in 17 CFR Parts 229, 232, 239, 240, and 249

Reporting and record keeping requirements, Securities.

For the reasons set forth in the preamble, the Commission is proposing to amend title 17, chapter II of the Code of Federal Regulations as follows:

PART 229—STANDARD INSTRUCTIONS FOR FILING FORMS UNDER SECURITIES ACT OF 1933, SECURITIES EXCHANGE ACT OF 1934 AND ENERGY POLICY AND CONSERVATION ACT OF 1975—REGULATION S–K

■ 1. The authority citation for part 229 continues to read as follows:

Authority: 15 U.S.C. 77e, 77f, 77g, 77h, 77j, 77k, 77s, 77z–2, 77z–3, 77aa(25), 77aa(26), 77ddd, 77eee, 77ggg, 77hhh, 77iii, 77jjj, 77nnn, 77sss, 78c, 78i, 78j, 78j–3, 78*l,* 78m, 78n, 78n–1, 78o, 78u–5, 78w, 78*ll,* 78mm, 80a–8, 80a–9, 80a–20, 80a–29, 80a–30, 80a–31(c), 80a–37, 80a–38(a), 80a–39, 80b–11 and 7201 *et seq.;* 18 U.S.C. 1350; sec. 953(b), Pub. L. 111–203, 124 Stat. 1904 (2010); and sec. 102(c), Pub. L. 112–106, 126 Stat. 310 (2012).

■ 2. Add § 229.106 to read as follows:

§ 229.106 (Item 106) Cybersecurity.

(a) *Definitions.* For purposes of this section:

Cybersecurity incident means 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.

Cybersecurity threat means any potential occurrence that may result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

Information systems means 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.

(b) *Risk management and strategy.* Disclose in such detail as necessary to adequately describe the registrant's policies and procedures, if it has any, for the identification and management of risks from cybersecurity threats, including, but not limited to: Operational risk (*i.e.,* disruption of business operations); intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk. Disclosure under this section should include, as applicable, a discussion of whether:

(1) The registrant has a cybersecurity risk assessment program, and if so, provide a description of such program;

(2) The registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program;

(3) The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider, including, but not limited to, those providers that have access to the registrant's customer and employee data. If so, the registrant shall describe these policies and procedures, including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers;

(4) The registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents, and if so, provide a description of the types of activities undertaken;

(5) The registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;

(6) Previous cybersecurity incidents informed changes in the registrant's governance, policies and procedures, or technologies;

(7) Cybersecurity-related risks and previous cybersecurity-related incidents have affected or are reasonably likely to affect the registrant's strategy, business model, results of operations, or financial condition and if so, how; and

(8) Cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation, and if so, how.

(c) *Governance.* (1) Describe the board's oversight of cybersecurity risk, including the following as applicable:

(i) Whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks;

(ii) The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and

(iii) Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

(2) Describe management's role in assessing and managing cybersecurity-related risks, as well as its role in implementing the registrant's cybersecurity policies, procedures, and strategies. The description should include, but not be limited to, the following information:

(i) Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

(ii) Whether the registrant has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart, and the relevant expertise of any such persons in such detail as necessary to fully describe the nature of the expertise;

(iii) The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and

(iv) Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

Instructions to Item 106(c): 1. In the case of a foreign private issuer with a two-tier board of directors, for purposes of paragraph (c) of this section, the term board of directors means the supervisory or non-management board. In the case of a foreign private issuer meeting the requirements of § 240.10A–3(c)(3) of this chapter, for purposes of paragraph (c) of this Item, the term board of directors means the issuer's board of auditors (or similar body) or statutory auditors, as applicable.

2. Relevant experience of management in Item 106(c)(2)(i) and (ii) may include, for example: Prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.

(d) *Updated incident disclosure.* (1) If the registrant has previously provided disclosure regarding one or more cybersecurity incidents pursuant to Item 1.05 of Form 8–K, the registrant must disclose any material changes, additions, or updates regarding such incident in the registrant's quarterly report filed with the Commission on Form 10–Q (17 CFR 249.308a) or annual report filed with the Commission on Form 10–K (17 CFR 249.310) for the period (the registrant's fourth fiscal quarter in the case of an annual report) in which the change, addition, or update occurred. The description should also include, as applicable, but not be limited to, the following information:

(i) Any material effect of the incident on the registrant's operations and financial condition;

(ii) Any potential material future impacts on the registrant's operations and financial condition;

(iii) Whether the registrant has remediated or is currently remediating the incident; and

(iv) 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.

(2) The registrant should provide the following disclosure to the extent known to management when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate:

(i) A general description of when the incidents were discovered and whether they are ongoing;

(ii) A brief description of the nature and scope of the incidents;

(iii) Whether any data was stolen or altered in connection with the incidents;

(iv) The effect of the incidents on the registrant's operations; and

(v) Whether the registrant has remediated or is currently remediating the incidents.

(e) *Structured Data Requirement.* Provide the information required by this Item in an Interactive Data File in accordance with Rule 405 of Regulation S–T and the EDGAR Filer Manual.

■ 3. Amend § 229.407 by adding paragraph (j) to read as follows:

§ 229.407 (Item 407) Corporate Governance.

* * * * *

(j) *Cybersecurity expertise.* (1) If any member of the registrant's board of directors has expertise in cybersecurity, disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise. In determining whether a director has expertise in cybersecurity, the registrant should consider, among other things:

(i) Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;

(ii) Whether the director has obtained a certification or degree in cybersecurity; and

(iii) Whether the director has 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.

(2) *Safe harbor.* (i) A person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including, without limitation, for purposes of Section 11 of the Securities Act (15 U.S.C. 77k), as a result of being designated or identified as a director with expertise in cybersecurity pursuant to this Item 407(j).

(ii) The designation or identification of a person as having expertise in cybersecurity pursuant to this Item 407(j) does not impose on such person any duties, obligations or liability that are greater than the duties, obligations and liability imposed on such person as a member of the board of directors in the absence of such designation or identification.

(iii) The designation or identification of a person as having expertise in cybersecurity pursuant to this Item 407(j) does not affect the duties, obligations, or liability of any other member of the board of directors.

(3) *Structured Data Requirement.* Provide the information required by this Item in an Interactive Data File in accordance with Rule 405 of Regulation S–T and the EDGAR Filer Manual.

* * * * *

Instruction to Item 407(j): In the case of a foreign private issuer with a two-tier board of directors, for purposes of paragraph (j) of this Item, the term board of directors means the supervisory or non-management board. In the case of a foreign private issuer meeting the requirements of § 240.10A–3(c)(3) of this chapter, for purposes of paragraph (j) of this Item, the term board of directors means the issuer's board of auditors (or similar body) or statutory auditors, as applicable.

* * * * *

■ 4. Amend § 229.601 by revising (b)(101)(i)(C)(*1*) as follows:

§ 229.601 (Item 601) Exhibits.

* * * * *

(b) * * *

(101) * * *

(i) * * *

(C) * * *

(*1*) Only when:

(*i*) The Form 8–K contains audited annual financial statements that are a revised version of financial statements that previously were filed with the Commission and that have been revised pursuant to applicable accounting standards to reflect the effects of certain subsequent events, including a discontinued operation, a change in reportable segments or a change in accounting principle. In such case, the Interactive Data File will be required only as to such revised financial statements regardless of whether the Form 8–K contains other financial statements; or

(*ii*) The Form 8–K includes disclosure required to be provided in an Interactive Data File pursuant to Item 1.05(b) of Form 8–K;

* * * * *

PART 232—REGULATION S–T—GENERAL RULES AND REGULATIONS FOR ELECTRONIC FILINGS

■ 5. The general authority citation for part 232 continues to read as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s(a), 77z–3, 77sss(a), 78c(b), 78l, 78m, 78n, 78o(d), 78w(a), 78ll, 80a–6(c), 80a–8, 80a–29, 80a–30, 80a–37, 7201 *et seq.*; and 18 U.S.C. 1350, unless otherwise noted.

■ 6. Amend § 232.405 by adding paragraphs (b)(1)(iii) and (b)(4) to read as follows:

§ 232.405 Interactive Data File submissions.

* * * * *

(b) * * *

(1) * * *

(iii) The disclosure set forth in paragraph (4) of this section, as applicable.

* * * * *

(4) An Interactive Data File must consist of the disclosure provided under 17 CFR 229 (Regulation S–K) and related provisions that is required to be tagged, including, as applicable:

(i) The cybersecurity information required by:

(A) Item 106 of Regulation S–K (§ 229.106 of this chapter);

(B) Item 407(j) of Regulation S–K (§ 229.407(j) of this chapter);

(C) Item 1.05 of Form 8–K (§ 249.308 of this chapter); and

(D) Item 16J of Form 20–F (§ 249.220f of this chapter).

* * * * *

PART 239—FORMS PRESCRIBED UNDER THE SECURITIES ACT OF 1933

■ 7. The authority citation for part 239 continues to read in part as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s, 77z–2, 77z–3, 77sss, 78c, 78*l,* 78m,78n, 78o(d), 78o–7 note, 78u–5, 78w(a), 78*ll,* 78mm, 80a–2(a), 80a–3, 80a–8, 80a–9, 80a–10, 80a–13, 80a–24, 80a–26, 80a–29, 80a–30, and 80a–37; and sec. 107, Pub. L. 112–106, 126 Stat. 312, unless otherwise noted.

■ 8. Amend § 239.13 by revising paragraph (a)(3)(ii) to read as follows:

§ 239.13 Form S–3, for registration under the Securities Act of 1933 of securities of certain issuers offered pursuant to certain types of transactions.

* * * * *

(a) * * *

(3) * * *

(ii) Has filed in a timely manner all reports required to be filed during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement, other than a report that is required solely pursuant to Item 1.01, 1.02, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a), 6.01, 6.03 or 6.05 of Form 8–K (§ 249.308 of this chapter). If the registrant has used (during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement) § 240.12b–25(b) of this chapter with respect to a report or a

portion of a report, that report or portion thereof has actually been filed within the time period prescribed by that section; and

* * * * *

■ 9. Amend Form S–3 (referenced in § 239.13) by adding General Instruction I.A.3(b) to read as follows:

Note: The text of Form S–3 does not, and this amendment will not, appear in the Code of Federal Regulations.

FORM S–3

* * * * *

INFORMATION TO BE INCLUDED IN THE REPORT

* * * * *

General Instructions

I. Eligibility Requirements for Use of Form S–3

* * * * *

A. Registrant Requirements.

* * * * *

3. * * *

(a) * * *

(b) has filed in a timely manner all reports required to be filed during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement, other than a report that is required solely pursuant to Item 1.01, 1.02, 1.04, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a) or 5.02(e) of Form 8–K (§ 249.308 of this chapter). If the registrant has used (during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement) Rule 12b–25(b) (§ 240.12b–25(b) of this chapter) under the Exchange Act with respect to a report or a portion of a report, that report or portion thereof has actually been filed within the time period prescribed by that rule.

* * * * *

■ 10. Amend § 239.45 by revising paragraph (a)(2) to read as follows:

§ 239.45 Form SF–3, for registration under the Securities Act of 1933 for offerings of asset-backed issuers offered pursuant to certain types of transactions.

* * * * *

(a) * * *

(2) To the extent the depositor or any issuing entity previously established, directly or indirectly, by the depositor or any affiliate of the depositor (as defined in Item 1101 of Regulation AB (17 CFR 229.1101)) is or was at any time during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement on this Form subject to the requirements of section 12 or 15(d) of the Exchange Act (15 U.S.C. 78*l* or 78o(d)) with respect to a class of asset-backed securities involving the same asset class, such depositor and each such issuing entity must have filed all material required to be filed regarding such asset-backed securities pursuant to section 13 or 15(d) of the Exchange Act (15 U.S.C. 78m or 78o(d)) for such period (or such shorter period that each such entity was required to file such materials). In addition, such material must have been filed in a timely manner, other than a report that is required solely pursuant to Item 1.01, 1.02, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a), 6.01, or 6.03 of Form 8–K (17 CFR 249.308). If § 240.12b–25(b) of this chapter was used during such period with respect to a report or a portion of a report, that report or portion thereof has actually been filed within the time period prescribed by § 240.12b–25(b) of this chapter. Regarding an affiliated depositor that became an affiliate as a result of a business combination transaction during such period, the filing of any material prior to the business combination transaction relating to asset-backed securities of an issuing entity previously established, directly or indirectly, by such affiliated depositor is excluded from this section, provided such business combination transaction was not part of a plan or scheme to evade the requirements of the Securities Act or the Exchange Act. See the definition of ''affiliate'' in § 230.405 of this chapter.

* * * * *

■ 11. Amend Form SF–3 (referenced in § 239.45) by revising General Instruction I.A(2) to read as follows:

Note: The text of Form SF–3 does not, and this addition will not, appear in the Code of Federal Regulations.

FORM SF–3

* * * * *

GENERAL INSTRUCTIONS

I. Eligibility Requirements for Use of Form SF–3

A.

(2) To the extent the depositor or any issuing entity previously established, directly or indirectly, by the depositor or any affiliate of the depositor (as defined in Item 1101 of Regulation AB (17 CFR 229.1101)) is or was at any time during the twelve calendar months and any portion of a month immediately preceding the filing of the registration statement on this Form subject to the requirements of section 12 or 15(d) of the Exchange Act (15 U.S.C. 78(l) or 78o(d)) with respect to a class of asset-backed securities involving the same asset class, such depositor and each such issuing entity must have filed all material required to be filed regarding such asset-backed securities pursuant to section 13 or 15(d) of the Exchange Act (15 U.S.C. 78m or 78o(d)) for such period (or such shorter period that each such entity was required to file such materials). In addition, such material must have been filed in a timely manner, other than a report that is required solely pursuant to Item 1.01, 1.02, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a), 6.01, or 6.03 of Form 8–K (17 CFR 249.308). If Rule 12b–25(b) (17 CFR 240.12b–25(b)) under the Exchange Act was used during such period with respect to a report or a portion of a report, that report or portion thereof has actually been filed within the time period prescribed by that rule. Regarding an affiliated depositor that became an affiliate as a result of a business combination transaction during such period, the filing of any material prior to the business combination transaction relating to asset-backed securities of an issuing entity previously established, directly or indirectly, by such affiliated depositor is excluded from this section, provided such business combination transaction was not part of a plan or scheme to evade the requirements of the Securities Act or the Exchange Act. See the definition of ''affiliate'' in Securities Act Rule 405 (17 CFR 230.405).

* * * * *

PART 240—GENERAL RULES AND REGULATIONS, SECURITIES EXCHANGE ACT OF 1934

■ 12. The authority citation for part 240 continues to read, in part, as follows:

Authority: 15 U.S.C. 77c, 77d, 77g, 77j, 77s, 77z–2, 77z–3, 77eee, 77ggg, 77nnn, 77sss, 77ttt, 78c, 78c–3, 78c–5, 78d, 78e, 78f, 78g, 78i, 78j, 78j–1, 78k, 78k–1, 78*l,* 78m, 78n, 78n–1, 78o, 78o–4, 78o–10, 78p, 78q, 78q–1, 78s, 78u–5, 78w, 78x, 78dd, 78*ll,* 78mm, 80a–20, 80a–23, 80a–29, 80a–37, 80b–3, 80b–4, 80b–11, and 7201 *et seq.,* and 8302; 7 U.S.C. 2(c)(2)(E); 12 U.S.C. 5221(e)(3); 18 U.S.C. 1350; Pub. L. 111–203, 939A, 124 Stat. 1376 (2010); and Pub. L. 112–106, sec. 503 and 602, 126 Stat. 326 (2012), unless otherwise noted.

* * * * *

Section 240.15d–11 is also issued under secs. 3(a) and 306(a), Pub. L. 107–204, 116 Stat. 745.

* * * * *

■ 13. Amend § 240.13a–11 by revising paragraph (c) to read as follows:

§ 240. 13a–11 Current reports on Form 8–K (§ 249.308 of this chapter).

* * * * *

(c) No failure to file a report on Form 8–K that is required solely pursuant to Item 1.01, 1.02, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a), 5.02(e) or 6.03 of Form 8–K shall be deemed to be a violation of 15 U.S.C. 78j(b) and § 240.10b–5.

■ 14. Amend § 240.15d–11 by revising paragraph (c) to read as follows:

§ 240.15d–11 Current reports on Form 8–K (§ 249.308 of this chapter).

* * * * *

(c) No failure to file a report on Form 8–K that is required solely pursuant to Item 1.01, 1.02, 1.05, 2.03, 2.04, 2.05, 2.06, 4.02(a), 5.02(e) or 6.03 of Form 8–K shall be deemed to be a violation of 15 U.S.C. 78j(b) and § 240.10b–5.

PART 249—FORMS, SECURITIES EXCHANGE ACT OF 1934

■ 15. The authority citation for part 249 continues to read, in part, as follows:

Authority: 15 U.S.C. 78a *et seq.* and 7201 *et seq.;* 12 U.S.C. 5461 *et seq.;* 18 U.S.C. 1350; Sec. 953(b), Pub. L. 111–203, 124 Stat. 1904; Sec. 102(a)(3), Pub. L. 112–106, 126 Stat. 309 (2012); Sec. 107, Pub. L. 112–106, 126 Stat. 313 (2012), Sec. 72001, Pub. L. 114–94, 129 Stat. 1312 (2015), and secs. 2 and 3 Pub. L. 116–222, 134 Stat. 1063 (2020), unless otherwise noted.

* * * * *

Section 249.220f is also issued under secs. 3(a), 202, 208, 302, 306(a), 401(a), 401(b), 406 and 407, Pub. L. 107–204, 116 Stat. 745, and secs. 2 and 3, Pub. L. 116–222, 134 Stat. 1063.

* * * * *

Section 249.308 is also issued under 15 U.S.C. 80a–29 and 80a–37.

Section 249.308a is also issued under secs. 3(a) and 302, Pub. L. 107–204, 116 Stat. 745.

* * * * *

Section 249.310 is also issued under secs. 3(a), 202, 208, 302, 406 and 407, Pub. L. 107–204, 116 Stat. 745.

* * * * *

■ 16. Amend Form 20–F (referenced in § 249.220f) by adding Item 16J to read as follows:

Note: The text of Form 20–F does not, and these amendments will not, appear in the Code of Federal Regulations.

FORM 20–F

* * * * *

PART II

* * * * *

Item 16J. Cybersecurity

(a) Definitions. For purposes of this section:

(1) *Cybersecurity incident* means 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.

(2) *Cybersecurity threat* means any potential occurrence that may result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

(3) *Information systems* means 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.

(b) *Risk management and strategy.*

(1) Disclose in such detail as necessary to adequately describe the registrant's policies and procedures, if it has any, for the identification and management of risks from cybersecurity threats, including, but not limited to: Operational risk (*i.e.,* disruption of business operations); intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk. Disclosure under this section should include, as applicable, a discussion of whether:

(i) The registrant has a cybersecurity risk assessment program, and if so, provide a description of such program;

(ii) The registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program;

(iii) The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider, including, but not limited to, those providers that have access to or have information about the registrant's customer and employee data. If so, the registrant shall describe these policies and procedures, including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers;

(iv) The registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents, and if so, provide a description of the types of activities undertaken;

(v) The registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;

(vi) Previous cybersecurity incidents informed changes in the registrant's governance, policies and procedures, or technologies;

(vii) Cybersecurity related risks and previous cybersecurity related incidents have affected or are reasonably likely to affect the registrant's strategy, business model, results of operations, or financial condition and if so, how; and

(viii) Cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation, and if so, how.

(c) *Governance.*

(1) Describe the board's oversight of cybersecurity risk, including the following as applicable:

(i) Whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks;

(ii) The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and

(iii) Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

(2) Describe management's role in assessing and managing cybersecurity related risks, as well as its role in implementing the registrant's cybersecurity policies, procedures, and strategies. The description should include, but not be limited to, the following information:

(i) Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

(ii) Whether the registrant has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart, and the relevant expertise of any such person in such detail as necessary to fully describe the nature of the expertise;

(iii) The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and

(iv) Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

Instructions to Item 16J(c)

1. In the case of a foreign private issuer with a two-tier board of directors, for purposes of paragraph (c) of this Item, the term board of directors means the supervisory or non-management board. In the case of a foreign private issuer meeting the requirements of § 240.10A–3(c)(3) of this chapter, for purposes of paragraph (c) of this Item, the term board of directors means the issuer's board of auditors (or similar body) or statutory auditors, as applicable.

2. Relevant experience of management in Item 16J(c)(2)(i) and (ii) may include, for example: Prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.

(d) *Updated incident disclosure.*

(1) If the registrant has previously provided disclosure regarding one or more cybersecurity incidents pursuant to Form 6–K, the registrant must disclose any material changes, additions, or updates regarding such incident that occurred during the reporting period. The description should also include, as applicable, but not limited to, the following information:

(i) Any material effect of the incident on the registrant's operations and financial condition;

(ii) Any potential material future impacts on the registrant's operations and financial condition;

(iii) Whether the registrant has remediated or is currently remediating the incident; and

(iv) 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.

(2) The registrant should provide the following disclosure to the extent known to management regarding any previously undisclosed material cybersecurity incidents that have occurred during the reporting period, including a series of individually immaterial cybersecurity incidents that have become material in the aggregate:

(i) A general description of when the incidents were discovered and whether they are ongoing;

(ii) A brief description of the nature and scope of the incidents;

(iii) Whether any data was stolen or altered in connection with the incidents;

(iv) The effect of the incidents on the registrant's operations; and

(v) Whether the registrant has remediated or is currently remediating the incidents.

(e) *Cybersecurity expertise.*

(1) If any member of the registrant's board of directors has expertise in cybersecurity, disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise. In determining whether a director has expertise in cybersecurity, the registrant should consider, among other things:

(i) Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;

(ii) Whether the director has obtained a certification or degree in cybersecurity; and

(iii) Whether the director has 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.

(2) *Safe harbor.*

(i) A person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including, without limitation, for purposes of Section 11 of the Securities Act (15 U.S.C. 77k), as a result of being designated or identified as a director with expertise in cybersecurity pursuant to this Item 16J.

(ii) The designation or identification of a person as having expertise in cybersecurity pursuant to this Item 16J does not impose on such person any duties, obligations or liability that are greater than the duties, obligations and liability imposed on such person as a member of the board of directors in the absence of such designation or identification.

(iii) The designation or identification of a person as having expertise in cybersecurity pursuant to this Item 16J does not affect the duties, obligations or liability of any other member of the board of directors.

(f) *Structured Data Requirement.* Provide the information required by this Item in an Interactive Data File in accordance with Rule 405 of Regulation S–T and the EDGAR Filer Manual.

Instruction to Item 16J. Item 16J applies only to annual reports, and does not apply to registration statements on Form 20–F.

* * * * *

■ 17. Amend Form 6–K (referenced in § 249.306) by adding the phrase ''cybersecurity incident'' before the phrase ''and any other information which the registrant deems of material importance to security holders.'' in the second paragraph of General Instruction B.

■ 18. Amend Form 8–K (referenced in § 249.308) by:

■ a. Revising General Instruction B.1.; and

■ b. Adding Item 1.05.

The revision and addition read as follows:

Note: The text of Form 8–K does not, and this addition will not, appear in the Code of Federal Regulations.

FORM 8–K

* * * * *

GENERAL INSTRUCTIONS

* * * * *

Instruction B. Events To Be Reported and Time for Filing of Reports

1. A report on this form is required to be filed or furnished, as applicable, upon the occurrence of any one or more of the events specified in the items in Sections 1 through 6 and 9 of this form. Unless otherwise specified, a report is to be filed or furnished within four business days after occurrence of the event. If the event occurs on a Saturday, Sunday or holiday on which the Commission is not open for business, then the four business day period shall begin to run on, and include, the first business day thereafter. A registrant either furnishing a report on this form under Item 7.01 (Regulation FD Disclosure) or electing to file a report on this form under Item 8.01 (Other Events) solely to satisfy its obligations under Regulation FD (17 CFR 243.100 and 243.101) must furnish such report or make such filing, as applicable, in accordance with the requirements of Rule 100(a) of Regulation FD (17 CFR 243.100(a)), including the deadline for furnishing or filing such report. A report pursuant to Item 5.08 is to be filed within four business days after the registrant determines the anticipated meeting date. A report pursuant to Item 1.05 is to be filed within four business days after the registrant determines that it has experienced a material cybersecurity incident.

* * * * *

Item 1.05 Cybersecurity Incidents

(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, disclose the following information to the extent known to the registrant at the time of filing:

(1) When the incident was discovered and whether it is ongoing;

(2) A brief description of the nature and scope of the incident;

(3) Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;

(4) The effect of the incident on the registrant's operations; and

(5) Whether the registrant has remediated or is currently remediating the incident.

(b) A registrant shall provide the information required by this Item in an Interactive Data File in accordance with Rule 405 of Regulation S–T and the EDGAR Filer Manual.

Instructions to Item 1.05

1. A registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident.

2. Disclosure of any material changes or updates to information disclosed pursuant to this Item 1.05 is required pursuant to § 229.106(d) [Item 106(d) of Regulation S–K] in the registrant's quarterly report filed with the Commission on Form 10–Q (17 CFR 249.308a) or annual report filed with the Commission on Form 10–K (17 CFR 249.310) for the period (the registrant's fourth fiscal quarter in the case of an annual report) in which the change, addition, or update occurred.

3. The definition of the term ''cybersecurity incident'' in § 229.106(a) [Item 106(a) of Regulation S–K] shall apply to this Item.

* * * * *

■ 19. Amend Form 10–Q (referenced in § 249.308(a) by:

■ a. Redesignating Item 5(b) as Item 5(c); and

■ b. Adding new Item 5(b) to read as follows:

Note: The text of Form 10–Q does not, and these amendments will not, appear in the Code of Federal Regulations.

FORM 10–Q

* * * * *

PART II—OTHER INFORMATION

* * * * *

Item 5. Other Information

* * * * *

(b) Furnish the information required by Item 106(d) of Regulation S–K (§ 229.106(d) of this chapter).

* * * * *

■ 20. Amend Form 10–K (referenced in § 249.310) by:

■ a. Adding Item 1.C to Part I; and

■ b. Revising Item 10 in Part III.

The addition and revision read as follows:

Note: The text of Form 10–K does not, and these amendments will not, appear in the Code of Federal Regulations.

FORM 10–K

* * * * *

PART I

* * * * *

Item 1.C. Cybersecurity

(a) Furnish the information required by Item 106 of Regulation S–K (§ 229.106 of this chapter).

(b) An asset-backed issuer as defined in Item 1101 of Regulation AB (§ 229.1101 of this chapter) that does not have any executive officers or directors may omit the information required by Item 106(c) of Regulation S–K (§ 229.106(c) of this chapter).

* * * * *

Item 10. Directors, Executive Officers and Corporate Governance. Furnish the information required by Items 401, 405, 406, and 407(c)(3), (d)(4), (d)(5), and (j) of Regulation S–K (§§ 229.401, 229.405, 229.406, and 229.407(c)(3), (d)(4), (d)(5), and (j) of this chapter).

* * * * *

By the Commission.

Dated: March 9, 2022.

Vanessa A. Countryman,

Secretary.

[FR Doc. 2022–05480 Filed 3–22–22; 8:45 am]

BILLING CODE 8011–01–P