Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

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

[Release Nos. 33-11216; 34-97989; File No. S7-09-22]

RIN 3235-AM89

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

SUMMARY: The Securities and Exchange Commission ("Commission") is adopting new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are adopting amendments to require current disclosure about material cybersecurity incidents. We are also adopting rules requiring periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks. Lastly, the final rules require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language ("Inline XBRL").

DATES: *Effective date*: The amendments are effective September 5, 2023.

Compliance dates: See Section II.I (Compliance Dates).

FOR FURTHER INFORMATION CONTACT: Nabeel Cheema, Special Counsel, at (202) 551-3430, in the Office of Rulemaking, Division of Corporation Finance; and, with respect to the application of the rules 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 adopting amendments to:

Commission Reference		**CFR Citation (17 CFR)**
Regulation S-K		§§ 229.10 through 229.1305
	Items 106 and 601	§§ 229.106 and 229.601
Regulation S-T		§§ 232.10 through 232.903
	Rule 405	§ 232.405
Securities Act of 1933 ("Securities Act")[1]	Form S-3	§ 239.13
Securities Exchange Act of 1934 ("Exchange Act")[2]	Rule 13a-11	§ 240.13a-11
	Rule 15d-11	§ 240.15d-11
	Form 20-F	§ 249.220f
	Form 6-K	§ 249.306
	Form 8-K	§ 249.308
	Form 10-K	§ 249.310

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

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

Table of Contents

I. Introduction and Background

On March 9, 2022, the Commission proposed new rules, and rule and form amendments, to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incidents by public companies that are subject to the reporting requirements of the Exchange Act.[3] The proposal followed on interpretive guidance on the application of existing disclosure requirements to cybersecurity risk and incidents that the Commission and staff had issued in prior years.

In particular, in 2011, the Division of Corporation Finance issued interpretive guidance providing the Division's views concerning operating companies' disclosure obligations relating to cybersecurity ("2011 Staff Guidance").[4] In that guidance, the staff observed that "[a]lthough no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents," and further that "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."[5] The guidance pointed specifically to disclosure obligations under 17 CFR 229.503 (Regulation S-K "Item 503(c)") (Risk factors) (since moved to 17 CFR 229.105 (Regulation S-K "Item 105")), 17 CFR 229.303 (Regulation S-K "Item 303") (Management's discussion and analysis of financial condition and results of operations), 17 CFR 229.101 (Regulation S-K "Item 101") (Description of business), 17 CFR 229.103 (Regulation S-K "Item 103") (Legal proceedings), and 17 CFR 229.307

---

3 *See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release No. 33-11038 (Mar. 9, 2022) [87 FR 16590 (Mar. 23, 2022)] ("Proposing Release").

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

5 *Id.*

(Disclosure controls and procedures), as well as to Accounting Standards Codifications 350-40 (Internal-Use Software), 605-50 (Customer Payments and Incentives), 450-20 (Loss Contingencies), 275-10 (Risks and Uncertainties), and 855-10 (Subsequent Events).[6]

In 2018, "[i]n light of the increasing significance of cybersecurity incidents," the Commission issued interpretive guidance to reinforce and expand upon the 2011 Staff Guidance and also address the importance of cybersecurity policies and procedures, as well as the application of insider trading prohibitions in the context of cybersecurity ("2018 Interpretive Release").[7] In addition to discussing the provisions previously covered in the 2011 Staff Guidance, the new guidance addressed 17 CFR 229.407 (Regulation S-K "Item 407") (Corporate Governance), 17 CFR Part 210 ("Regulation S-X"), and 17 CFR Part 243 ("Regulation FD").[8] The 2018 Interpretive Release noted that companies can provide current reports on Form 8-K and Form 6-K to maintain the accuracy and completeness of effective shelf registration statements, and it also advised companies to consider whether it may be appropriate to implement restrictions on insider trading during the period following an incident and prior to disclosure.[9]

As noted in the Proposing Release, current disclosure practices are varied. For example, while some registrants do report material cybersecurity incidents, most typically on Form 10-K, review of Form 8-K, Form 10-K, and Form 20-F filings by staff in the Division of Corporation Finance has shown that companies provide different levels of specificity regarding the cause, scope, impact, and materiality of cybersecurity incidents. Likewise, staff has also observed that,

---

6 *Id.*

7 *See Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release No. 33-10459 (Feb. 21, 2018) [83 FR 8166 (Feb. 26, 2018)], at 8167.

8 *Id.*

9 *Id.*

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 included with other unrelated disclosures, which makes it more difficult for investors to locate, interpret, and analyze the information provided.[10]

In the Proposing Release, the Commission explained that a number of trends underpinned investors' and other capital markets participants' need for more timely and reliable information related to registrants' cybersecurity than was produced following the 2011 Staff Guidance and the 2018 Interpretive Release. First, an ever-increasing share of economic activity is dependent on electronic systems, such that disruptions to those systems can have significant effects on registrants and, in the case of large-scale attacks, systemic effects on the economy as a whole.[11] Second, there has been a substantial rise in the prevalence of cybersecurity incidents, propelled by several factors: the increase in remote work spurred by the COVID-19 pandemic; the increasing reliance on third-party service providers for information technology services; and the rapid monetization of cyberattacks facilitated by ransomware, black markets for stolen data, and crypto-asset technology.[12] Third, the costs and adverse consequences of cybersecurity incidents to companies are increasing; such costs include business interruption, lost revenue, ransom payments, remediation costs, liabilities to affected parties, cybersecurity protection costs, lost assets, litigation risks, and reputational damage.[13]

---

[10] *See infra* Section IV.A (noting that current cybersecurity disclosures appear in varying sections of companies' periodic and current reports and are sometimes included with other unrelated disclosures).

[11] Proposing Release at 16591-16592. *See also* U.S. FINANCIAL STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT (2021), at 168, *available at https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf* (finding that "a destabilizing cybersecurity incident could potentially threaten the stability of the U.S. financial system").

[12] Proposing Release at 16591-16592.

[13] *Id.*

Since publication of the Proposing Release, these trends have continued apace, with significant cybersecurity incidents occurring across companies and industries. For example, threat actors repeatedly and successfully executed attacks on high-profile companies across multiple critical industries over the course of 2022 and the first quarter of 2023, causing the Department of Homeland Security's Cyber Safety Review Board to initiate multiple reviews.[14] Likewise, state actors have perpetrated multiple high-profile attacks, and recent geopolitical instability has elevated such threats.[15] A recent study by two cybersecurity firms found that 98 percent of organizations use at least one third-party vendor that has experienced a breach in the last two years.[16] In addition, recent developments in artificial intelligence may exacerbate cybersecurity threats, as researchers have shown that artificial intelligence systems can be leveraged to create code used in cyberattacks, including by actors not versed in programming.[17] Overall, evidence suggests companies may be underreporting cybersecurity incidents.[18]

---

[14] *See* Department of Homeland Security, *Cyber Safety Review Board to Conduct Second Review on Lapsus$* (Dec. 2, 2022), *available at https://www.dhs.gov/news/2022/12/02/cyber-safety-review-board-conduct-second-review-lapsus*; *see also* Tim Starks, *The Latest Mass Ransomware Attack Has Been Unfolding For Nearly Two Months*, WASH. POST (Mar. 27, 2023), *available at https://www.washingtonpost.com/politics/2023/03/27/latest-mass-ransomware-attack-has-been-unfolding-nearly-two-months/*.

[15] *See*, *e.g.*, Press Release, Federal Bureau of Investigation, *FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft* (Jan. 23, 2023), *available at https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft*; Alert (AA22-257A), Cybersecurity & Infrastructure Security Agency, *Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations* (Sep. 14, 2022), *available at https://www.cisa.gov/uscert/ncas/alerts/aa22-257a*; National Security Agency et al., *Joint Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure* (Apr. 20, 2022), *available at https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/joint_csa_russian_state-sponsored_and_criminal_cyber_threats_to_critical_infrastructure_20220420.pdf*.

[16] SecurityScorecard, *Cyentia Institute and SecurityScorecard Research Report: Close Encounters of the Third (and Fourth) Party Kind* (Feb 1, 2023), *available at https://securityscorecard.com/research/cyentia-close-encounters-of-the-third-and-fourth-party-kind/*.

[17] Check Point Research, *OPWNAI: AI that Can Save the Day or Hack it Away* (Dec. 19, 2022), *available at https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away*.

[18] Bitdefender*, Whitepaper: Bitdefender 2023 Cybersecurity Assessment* (Apr. 2023), *available at https://businessresources.bitdefender.com/bitdefender-2023-cybersecurity-assessment*.

Legislatively, we note two significant developments occurred following publication of the Proposing Release. First, the President signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA")[19] on March 15, 2022, as part of the Consolidated Appropriations Act of 2022.[20] The centerpiece of CIRCIA is the reporting obligation placed on companies in defined critical infrastructure sectors.[21] Once rules are adopted by the Cybersecurity & Infrastructure Security Agency ("CISA"), these companies will be required to report covered cyber incidents to CISA within 72 hours of discovery, and report ransom payments within 24 hours.[22] Importantly, reports made to CISA pursuant to CIRCIA will remain confidential; while the information contained therein may be shared across Federal agencies for cybersecurity, investigatory, and law enforcement purposes, the information may not be disclosed publicly, except in anonymized form.[23] We note that CIRCIA also mandated the creation of a "Cyber Incident Reporting Council . . . to coordinate, deconflict, and harmonize Federal incident reporting requirements" (the "CIRC"), of which the Commission is a member.[24] Second, on December 21, 2022, the President signed into law the Quantum Computing Cybersecurity Preparedness Act, which directs the Federal Government to adopt technology that is protected from decryption by quantum computing, a developing technology that may increase

---

19 Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 1038 (2022).

20 Consolidated Appropriations Act of 2022, H.R. 2471, 117th Cong. (2022).

21 The sectors are defined in Presidential Policy Directive / PPD-21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), as: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; Water and Wastewater Systems. Because these sectors encompass some private companies and do not encompass all public companies, CIRCIA's reach is both broader and narrower than the set of companies subject to the rules we are adopting.

22 6 U.S.C. 681b(a)(1).

23 6 U.S.C. 681e. *See infra* Section II.A.3 for a discussion of why our final rules serve a different purpose and are not at odds with the goals of CIRCIA.

24 6 U.S.C. 681f.

computer processing capacity considerably and thereby render existing computer encryption vulnerable to decryption.[25]

We received over 150 comment letters in response to the Proposing Release.[26] The majority of comments focused on the proposed incident disclosure requirement, although we also received substantial comment on the proposed risk management, strategy, governance, and board expertise requirements. In addition, the Commission's Investor Advisory Committee adopted recommendations ("IAC Recommendation") with respect to the proposal, stating that it: supports the proposed incident disclosure requirement; supports the proposed risk management, strategy, and governance disclosure requirements; recommends the Commission reconsider the proposed board of directors' cybersecurity expertise disclosure requirement; suggests requiring companies to disclose the key factors they used to determine the materiality of a reported cybersecurity

---

[25] Quantum Computing Cybersecurity Preparedness Act, H.R. 7535, 117th Cong. (2022). More recently, the White House released a National Cybersecurity Strategy to combat the ongoing risks associated with cyberattacks. The National Cybersecurity Strategy seeks to rebalance the responsibility for defending against cyber threats toward companies instead of the general public, and looks to realign incentives to favor long-term investments in cybersecurity. *See* Press Release, White House, FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy (Mar. 2, 2023), *available at https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/*.

[26] The public comments we received are *available at https://www.sec.gov/comments/s7-09-22/s70922.htm*. On Mar. 9, 2022, the Commission published the Proposing Release on its website. The comment period for the Proposing Release was open for 60 days from issuance and publication on SEC.gov and ended on May 9, 2022. One commenter asserted that the comment period was not sufficient and asked the Commission to extend it by 30 days. *See* letter from American Chemistry Council ("ACC"). In Oct. 2022, the Commission reopened the comment period for the Proposing Release and other rulemakings because certain comments on the Proposing Release and other rulemakings were potentially affected by a technological error in the Commission's internet comment form. *See Resubmission of Comments and Reopening of Comment Periods for Several Rulemaking Releases Due to a Technological Error in Receiving Certain Comments*, Release No. 33-11117 (Oct. 7, 2022) [87 FR 63016 (Oct. 18, 2022)] ("Reopening Release"). The Reopening Release was published on the Commission's website on Oct. 7, 2022 and in the Federal Register on Oct. 18, 2022, and the comment period ended on Nov. 1, 2022. A few commenters asserted that the comment period for the reopened rulemakings was not sufficient and asked the Commission to extend the comment period for those rulemakings. *See, e.g.*, letters from Attorneys General of the states of Montana *et al.* (Oct. 24, 2022) and U.S. Chamber of Commerce (Nov. 1, 2022). We have considered all comments received since Mar. 9, 2022 and do not believe an additional extension of the comment period is necessary.

incident; and suggests extending the proposed 17 CFR 229.106 (Regulation S-K "Item 106") disclosure requirements to registration statements.[27]

We are making a number of important changes from the Proposing Release in response to comments received. With respect to incident disclosure, we are narrowing the scope of disclosure, adding a limited delay for disclosures that would pose a substantial risk to national security or public safety, requiring certain updated incident disclosure on an amended Form 8-K instead of Forms 10-Q and 10-K for domestic registrants, and on Form 6-K instead of Form 20-F for foreign private issuers ("FPIs"),[28] and omitting the proposed aggregation of immaterial incidents for materiality analyses. We are streamlining the proposed disclosure elements related to risk management, strategy, and governance, and we are not adopting the proposed requirement to disclose board cybersecurity expertise. The following table summarizes the requirements we are adopting, including changes from the Proposing Release, as described more fully in Section II below:[29]

---

[27] *See* U.S. Securities and Exchange Commission Investor Advisory Committee, Recommendation of the Investor as Owner Subcommittee and Disclosure Subcommittee of the SEC Investor Advisory Committee Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Sept. 21, 2022), *available at https://www.sec.gov/spotlight/investor-advisory-committee-2012/20220921-cybersecurity-disclosure-recommendation.pdf*. The Investor Advisory Committee also held a panel discussion on cybersecurity at its Mar. 10, 2022 meeting. *See* U.S. Securities and Exchange Commission Investor Advisory Committee, Meeting Agenda (Mar. 10, 2022), *available at https://www.sec.gov/spotlight/investor-advisory-committee/iac031022-agenda.htm*.

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

[29] The information in this table is not comprehensive and is intended only to highlight some of the more significant aspects of the final amendments. It does not reflect all of the amendments or all of the rules and forms that are affected by the final amendments, which are discussed in detail below. As such, this table should be read together with the entire release, including the regulatory text.

Item	**Summary Description of the Disclosure Requirement**[30]
Regulation S-K Item 106(b) – *Risk management and strategy*	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
Regulation S-K Item 106(c) – *Governance*	Registrants must: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 8-K Item 1.05 – *Material Cybersecurity Incidents*	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: - Nature, scope, and timing; and - Impact or reasonably likely impact. An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety. Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.
Form 20-F	FPIs must: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 6-K	FPIs must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise

[30] 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, which are a type of closed-end investment company that is not registered under the Investment Company Act, but do not include investment companies registered under that Act.

	publicize in a foreign jurisdiction, to any stock exchange, or to security holders.

Overall, we remain persuaded that, as detailed in the Proposing Release: under-disclosure regarding cybersecurity persists despite the Commission's prior guidance; investors need more timely and consistent cybersecurity disclosure to make informed investment decisions; and recent legislative and regulatory developments elsewhere in the Federal Government, including those developments subsequent to the issuance of the Proposing Release such as CIRCIA[31] and the Quantum Computing Cybersecurity Preparedness Act,[32] while serving related purposes, will not effectuate the level of public cybersecurity disclosure needed by investors in public companies.

II. Discussion of Final Amendments

A. Disclosure of Cybersecurity Incidents on Current Reports

1. Proposed Amendments

The Commission proposed to amend Form 8-K by adding new Item 1.05 that would require a registrant to disclose the following information regarding a material cybersecurity incident, to the extent known at the time of 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 were stolen, altered, accessed, or used for any other unauthorized purpose;
- The effect of the incident on the registrant's operations; and

[31] *Supra* note 19.

[32] *Supra* note 25.

- Whether the registrant has remediated or is currently remediating the incident.[33]

The Commission clarified in the Proposing Release that this requirement would not extend to specific, technical information about the registrant's 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.[34]

The Commission proposed to set the filing trigger for Item 1.05 as the date the registrant determines that a cybersecurity incident is material; as with all other Form 8-K items, the proposed filing deadline would be four business days after the trigger.[35] To protect against any inclination on the part of a registrant to delay making a materiality determination with a view toward prolonging the filing deadline, the Commission proposed adding Instruction 1 to Item 1.05 requiring that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."[36]

The Commission affirmed in the Proposing Release that the materiality standard registrants should apply in evaluating whether a Form 8-K would be triggered under proposed Item 1.05 would be consistent with that set out in the numerous cases addressing materiality in the securities laws, including *TSC Industries, Inc. v. Northway, Inc.*,[37] *Basic, Inc. v. Levinson*,[38] and *Matrixx Initiatives, Inc. v. Siracusano*,[39] and likewise with that set forth in 17 CFR 230.405 ("Securities Act Rule 405") and 17 CFR 240.12b-2 ("Exchange Act Rule 12b-2"). That is,

---

33 Proposing Release at 16595.

34 *Id.*

35 *Id*.

36 *Id.* at 16596.

37 *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976).

38 *Basic Inc. v. Levinson*, 485 U.S. 224, 232 (1988).

39 *Matrixx Initiatives v. Siracusano*, 563 U.S. 27 (2011).

information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important"[40] in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."[41] "Doubts as to the critical nature" of the relevant information should be "resolved in favor of those the statute is designed to protect," namely investors.[42]

The Commission explained that the timely disclosure of the information required by proposed Item 1.05 would enable investors and other market participants to assess the possible effects of a material cybersecurity incident on the registrant, including any short- and long-term financial effects or operational effects, resulting in information useful for their investment decisions.[43] Aligning the deadline for Item 1.05 with that of the other Form 8-K items would, the Commission maintained, significantly improve the timeliness of cybersecurity incident disclosures as well as standardize those disclosures.[44] The Commission did not propose to provide a reporting delay in cases of ongoing internal or external investigations of cybersecurity incidents.[45] Nevertheless, the Proposing Release requested comment on whether to allow a delay in reporting where the Attorney General determines that a delay is in the interest of national security.[46]

---

40 *TSC Indus.*, 426 U.S. at 449.

41 *Id.*

42 *Id.* at 448.

43 Proposing Release at 16595.

44 *Id*.

45 *Id.* at 16596.

46 *Id.* at 16598.

2. Comments

Proposed Item 1.05 received a significant amount of feedback from commenters. Some commenters supported Item 1.05 as proposed,[47] saying that the current level of disclosure on cybersecurity incidents is inadequate to meet investor needs, and Item 1.05 would remedy this inadequacy by effectuating the disclosure of decision-useful information.[48] One commenter also anticipated that Item 1.05 would reduce the risk of insider trading by shortening the time between discovery of an incident and public disclosure.[49]

Other commenters opposed proposed Item 1.05, for several reasons. Some commenters said that if proposed Item 1.05 were to result in disclosure while an incident is still ongoing, it would tip off the threat actor and thus make successful neutralization of the incident more difficult.[50] Commenters also expressed concern that public notice of a vulnerability could draw attacks from other threat actors who were previously unaware of the vulnerability; and such attacks could target the disclosing registrant or other companies with the same vulnerability, particularly if the vulnerability is with a third-party service provider used by multiple

---

47 *See* letters from American Institute of CPAs ("AICPA"); Better Markets ("Better Markets"); BitSight Technologies, Inc. ("BitSight"); California Public Employees' Retirement System ("CalPERS"); Crindata, LLC ("Crindata"); Council of Institutional Investors ("CII"); Information Technology and Innovation Foundation ("ITIF"); North American Securities Administrators Association Inc. ("NASAA"); Professor Jerry Perullo ("Prof. Perullo"); Professor Preeti Choudhary ("Prof. Choudhary"); Tessa Mishoe ("T. Mishoe"). *See also* IAC Recommendation.

48 *Id.*

49 *See* letter from Better Markets.

50 *See* letters from ACC; American Gas Association and Interstate Natural Gas Association of America ("AGA/INGAA"); BioTechnology Innovation Organization ("BIO"); Bank Policy Institute, American Bankers Association, and Mid-Size Bank Coalition of America ("BPI et al."); BSA / The Software Alliance ("BSA"); Business Roundtable ("Business Roundtable"); Canadian Bankers Association ("CBA"); Edison Electric Institute ("EEI"); Energy Infrastructure Council ("EIC"); Federation of American Hospitals ("FAH"); Financial Services Sector Coordinating Council ("FSSCC"); Information Technology Industry Council ("ITI"); LTSE Services, Inc. ("LTSE"); National Association of Manufacturers ("NAM"); National Defense Industrial Association ("NDIA"); Quest Diagnostics Incorporated ("Quest"); Rapid7, Inc. ("Rapid7"); Society for Corporate Governance ("SCG"); Securities Industry and Financial Markets Association ("SIFMA"); TransUnion; R Street Institute ("R Street"); U.S. Chamber of Commerce ("Chamber").

companies.[51] Some of these commenters objected specifically to the requirement in Item 1.05 to disclose whether remediation has occurred, stating that this information could assist threat actors in their targeting or invite further targeted attacks,[52] while others more generally stated that the Item 1.05 disclosure would be overly detailed, such that it would give a road map to threat actors for planning attacks.[53] One commenter argued that the prospect of possibly having to file an Item 1.05 Form 8-K could chill threat information sharing within industries, because companies would fear that any cybersecurity risk information they share could later be used to question their disclosure decisions.[54]

Some of the commenters that disagreed with the level of disclosure required by proposed Item 1.05 recommended that the Commission narrow the disclosure requirements of the rule. For example, one such commenter advised dropping the proposed requirement to disclose "when the incident was discovered," arguing that this detail may cause confusion, particularly where an incident was detected some time ago but a significant aspect rendering it material surfaced only recently.[55] Another commenter opined that "whether the registrant has remediated or is currently remediating the incident" is duplicative of "whether it is ongoing," so either of the two could be

---

[51] *See* letters from ABA Committee on Federal Regulation of Securities ("ABA"); Aerospace Industries Association of America ("AIA"); Alliance for Automotive Innovation ("Auto Innovators"); AGA/INGAA; American Property Casualty Insurance Association ("APCIA"); BPI et al.; BSA; Business Roundtable; CBA; Chamber; Cellular Telecommunications and Internet Assoc. ("CTIA"); Cybersecurity Coalition; EEI; EIC; Empire State Realty Trust, Inc. ("Empire"); Enbridge Inc. ("Enbridge"); FSSCC; Internet Security Alliance; ITI; Microsoft Corporation ("Microsoft"); NDIA; PPG Industries, Inc. ("PPG"); PricewaterhouseCoopers LLP ("PWC"); Rapid7; R Street; SCG; SIFMA; U.S. Senator Rob Portman ("Sen. Portman"); Virtu Financial ("Virtu").

[52] *See* letters from ABA; AGA/INGAA; BPI et al.; Cybersecurity Coalition; Empire; Enbridge; PWC; SIFMA; SCG; Virtu.

[53] *See* letters from AGA/INGAA; BSA; EIC; ITI; PPG.

[54] *See* letter from Consumer Technology Association ("CTA").

[55] *See* letter from Prof. Perullo.

eliminated.[56] One commenter contended that a materiality filter should be added to the details required by Item 1.05, such that companies would have to disclose only details that themselves are material, rather than immaterial details of a material incident.[57]

By contrast, there were also commenters that recommended expanding the disclosure requirements in the proposed rule. In this regard, some commenters recommended requiring that registrants disclose asset losses, intellectual property losses, and the value of business lost due to the incident.[58] Other suggestions included requiring that incidents be quantified as to their severity and impact via standardized rating systems, and that registrants disclose how they became aware of the incident, as this may shed light on the effectiveness of a company's cybersecurity policies and procedures.[59] Additionally, commenters suggested banning trading by insiders during the time between the materiality determination and disclosure of the incident.[60]

Commenters provided reactions to the application of Item 1.05 to incidents connected with third-party systems. A number of commenters contended that registrants should be exempt from having to disclose cybersecurity incidents in third-party systems they use because of their reduced control over such systems.[61] Similarly, several commenters advocated for a safe harbor for information disclosed about third-party systems, given registrants' reduced visibility into such systems.[62] A few commenters suggested a longer reporting timeframe for third-party

---

56 *See* letter from ABA.

57 *See* letter from ITI.

58 *See* letters from Profs. Rajgopal & Sharpe; PWC.

59 *See* letters from BitSight; Cloud Security Alliance ("CSA").

60 *See* letter from Prof. Mitts.

61 *See* letters from ABA; AIA; APCIA; Business Roundtable; Cybersecurity Coalition; Chamber; EIC; FAH; ISA; ITI; NAM; NDIA; National Multifamily Housing Council and National Apartment Association ("NMHC"); Paylocity; SIFMA.

62 *See* letters from Chevron Corporation ("Chevron"); APCIA; BPI et al.; BIO; CSA; Financial Executive International's Committee on Corporate Reporting ("FEI"); ITI; ISA; NMHC; SIFMA.

incidents, because the registrant may be dependent on the third party for information (which may not be provided in a timely manner), and to avoid harm to other companies reliant on the same third party.[63] Commenters also recommended that Item 1.05 be phased in over a longer period of time with respect to third-party incidents, to give registrants time to develop information sharing processes with their third-party service providers.[64]

Commenters also requested guidance or otherwise raised concerns where the proposed requirements might trigger disclosures *by* third-party service providers. A commenter requested clarity on whether an incident should be disclosed by the third-party service provider registrant that owns the affected system or the customer registrant that owns the affected information, or both.[65] And two commenters argued that third-party service providers should simply pass along information to their end customers, who would then make their own materiality determination and disclose accordingly; this should particularly be the case, a commenter said, where an attack on a third-party data center results in a data breach for an end customer but does not affect the services the data center provides.[66]

The proposed timing of incident disclosure also received a significant level of public comment. For example, a few commenters said the level of detail required by Item 1.05 is impractical to produce in the allotted time.[67] Other commenters said that the proposed deadline would lead to the disclosure of tentative, unclear, or potentially inaccurate information that is not

---

63 *See* letters from ABA; R Street.

64 *See* letters from Business Roundtable; Deloitte & Touche LLP ("Deloitte").

65 *See* letter from Business Roundtable.

66 *See* letters from BSA; ITI.

67 *See* letters from ABA; NMHC; Quest.

decision-useful to investors,[68] resulting in the market mispricing the underlying securities.[69] Commenters also argued that Item 1.05 is qualitatively different from all other Form 8-K items in that the trigger for Item 1.05 is largely outside the company's control.[70] Some commenters worried the proposed deadline would lead to disclosure of "false positives," that is, incidents that appear material at first but later on with the emergence of more information turn out not to be material.[71]

Commenters suggested a range of alternative reporting deadlines for Item 1.05. A common suggestion was to modify the measurement date from the determination of materiality to another point in the lifecycle of the incident when the incident is no longer a threat to the registrant—commenters variously termed this as "containment," "remediation," "mitigation," and comparable terms.[72] One commenter recommended conditioning a reporting delay on the registrant being actively engaged in containing the incident and reasonably believing that containment can be completed in a timely manner.[73] Similarly, several commenters recommended that the rule allow for a delay in providing Item 1.05 disclosure based on a registrant's assessment of the potential negative consequences of public disclosure, using a

---

68 *See* letters from ABA; ACC; AIA; Auto Innovators; American Investment Council ("AIC"); BIO; Business Roundtable; CBA; Chamber; Confidentiality Coalition; CTIA; Davis Polk & Wardwell LLP ("Davis Polk"); Debevoise & Plimpton ("Debevoise"); Federated Hermes; FSSCC; Microsoft; NAM; Nasdaq Stock Market, LLC ("Nasdaq"); NDIA; Quest; SCG; TransUnion; Wilson Sonsini Goodrich & Rosati ("Wilson Sonsini"); Virtu.

69 *See* letters from ABA; ACC; AIA; AIC; BIO; BPI et al.; Business Roundtable; Confidentiality Coalition; Davis Polk; ISA; Nasdaq; PPG; Quest; Rapid7; SCG; Sen. Portman; SIFMA; Virtu.

70 *See* letters from CTIA; Debevoise; EIC; LTSE; New York City Bar Association ("NYC Bar"); Quest.

71 *See* letters from LTSE; PPG; SCG.

72 *See* letters from American Council of Life Insurers ("ACLI"); BCE Inc., Rogers Communications Inc., TELUS Corporation ("BCE"); BPI et al.; Business Roundtable; Chamber; CTA; Cybersecurity Coalition; Empire; FAH; Federated Hermes; FSSCC; ISA; ITI; NAM; Nasdaq; NDIA; NMHC; NYSE Group ("NYSE"); Quest; Rapid7; Sen. Portman; SCG; SIFMA; SM4RT Secure LLC ("SM4RT Secure"); TransUnion.

73 *See* letter from Rapid7.

variety of measures they suggested.[74] Another suggestion was to replace the proposed deadline with an instruction to disclose material incidents "without unreasonable delay."[75]

Some commenters recommended instead increasing the number of days between the reporting trigger and the reporting deadline. A few commenters recommended adding one business day to make the deadline five business days;[76] one noted this would result in every registrant having at least a full calendar week to gather information and prepare the Form 8-K.[77] Another commenter recommended a deadline of 15 business days, along with a cure period to allow registrants a defined period of time to fix potential reporting mistakes.[78] A few commenters recommended a 30-day deadline,[79] with their choice of 30 days tending to be a proxy for some other factor, such as containment or remediation,[80] or state notification requirements.[81]

---

74 *See* letters from BSA (suggesting a "tailored, balancing test"); EEI (advocating delay "to the extent… the registrant in good faith concludes that its disclosure will expose it or others to ongoing or additional risks of a cybersecurity incident"); EIC; Microsoft (requesting that companies be allowed to "manage the timing" of disclosure "when compelling conditions exist such that premature disclosure would result in greater harm to the company, its investors, or the national digital ecosystem"); Nareit and The Real Estate Roundtable ("Nareit") (stating delay should be permitted where disclosure "would exacerbate injury to the company and/or its shareholders"); SIFMA (advocating a "'responsible disclosure' exception" that applies "where disclosure of a cyber incident or vulnerability could have a more damaging effect than delayed disclosure"); Wilson Sonsini (stating "the Commission should allow board members to decide to delay reporting if doing so could cause material harm to the company").

75 *See* letters from CTIA; National Restaurant Association ("NRA").

76 *See* letters from AIC; Debevoise; NYC Bar.

77 *See* letter from AIC.

78 *See* letter from R Street.

79 *See* letters from APCIA; Hunton Andrews Kurth, LLP ("Hunton"); Rapid7.

80 *See* letters from APCIA ("[w]e believe that permitting a registrant to delay the filing for a short period of time strikes an appropriate balance between timely disclosure to shareholders and an opportunity for a registrant to achieve the best resolution for itself and its shareholders"); Rapid7 ("[i]n Rapid7's experience, the vast majority of incidents can be contained and mitigated within that time frame [30 days]").

81 *See* letters from APCIA ("[a]llowing up to 30 days for disclosure would also bring the SEC's proposal in line with data breach disclosure requirements at the state level"); Hunton ("[w]hile state data breach notification laws vary from state to state, 30 days from the cybersecurity incident is the earliest date any state requires that notification to affected persons be made").

Several commenters recommended addressing the timing concerns by replacing current reporting on Form 8-K with periodic reporting on Forms 10-Q and 10-K, to allow additional time to assess an incident's impact before reporting to markets.[82] In this vein, one commenter likened cybersecurity incident disclosure to the disclosure of legal proceedings under Regulation S-K Item 103.[83]

A few commenters recommended instead that the materiality trigger be replaced with a quantifiable trigger; for example, an incident implicating a specified percentage of revenue, or the costs of an incident exceeding a specified benchmark, could trigger disclosure.[84] Other commenters advocated for the disclosure trigger to be tied to any legal obligation that forces a registrant to notify persons outside the company.[85]

Commenters also recommended a number of exceptions to the filing deadline. The most common recommendation was to include a provision allowing for delayed filing where there is an active law enforcement investigation or the disclosure otherwise implicates national security or public safety.[86] A representative comment in this vein advanced a provision whereby registrants may "delay reporting of a cybersecurity incident that is the subject of a *bona fide*

---

82 *See* letters from ABA; Davis Polk; Debevoise; LTSE; NYC Bar; Quest; SCG.

83 *See* letter from Quest.

84 *See* letters from BIO; Bitsight; EIC; Paylocity.

85 *See* letters from ABA; Business Roundtable.

86 *See* letters from ABA; ACC; ACLI; AGA/INGAA; AIA; AICPA; APCIA; Auto Innovators; Rep. Banks; BPI et al.; BIO; BSA; Business Roundtable; CBA; Chamber; Chevron; CII; CSA; CTA; CTIA; Cybersecurity Coalition; Debevoise; EEI; EIC; Empire; Enbridge; FAH; FedEx Corporation ("FedEx"); FEI; FSSCC; Global Privacy Alliance ("GPA"); Hunton; ISA; ITI; ITIF; Microsoft; NAM; Nareit; NASAA; NDIA; NMHC; NRA; NYC Bar; Prof. Perullo; Sen. Portman; PPG; PWC; Quest; R Street; Profs. Rajgopal & Sharpe; Rapid7; SCG; SIFMA; TransUnion; Virtu; USTelecom – The Broadband Association ("USTelecom"); U.S. Chamber of Commerce & various associations ("Chamber et al.").

investigation by law enforcement," because such "delay in reporting may not only facilitate such an investigation, it may be critical to its success."[87]

In calling for a law enforcement delay, associations for industries in critical sectors emphasized the national security implications of public cybersecurity incident disclosure. For example, one association explained that disclosure "may alert malicious actors that we have uncovered their illegal activities in circumstances where our defense and intelligence agencies wish to keep that information secret."[88] Likewise, another association pointed out that, in its industry, companies "are likely to possess some of the nation's most critical confidential information, including cybersecurity threat information furnished by government entities, such as the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the National Security Agency (NSA)," and therefore, disclosure may not be possible.[89]

Commenters largely advocated for "a broad law enforcement exception that applies not only in the interest of national security but also when law enforcement believes disclosure will hinder their efforts to identify or capture the threat actor."[90] Many commenters that responded to the Commission's request for comment regarding a provision whereby the Attorney General determines that a delay is in the interest of national security indicated that such a provision should be more expansive and extend to other law enforcement authorities.[91] One of these commenters questioned whether the Attorney General would opine on matters "that are under the ambit of other Federal agencies, such as the Department of Homeland Security, Department of

87 *See* letter from Debevoise.

88 *See* letter from AIA.

89 *See* letter from EEI.

90 *See* letter from ABA.

91 *See* letters from BPI et al.; CBA; CSA; Hunton; ITIF; SCG; Wilson Sonsini.

State and the Department of Defense."[92] Another commenter pointed out that "the Department of Justice is not the primary, or even the lead, organization in the Federal Government for cybersecurity response, rather the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency is often the first call that companies make," while "[f]or defense contractors, the Department of Defense is likely to have the highest interest in the timing of an announcement."[93] For the financial industry specifically, one suggestion was to permit a delay if the Federal Reserve, Federal Deposit Insurance Corporation, or Office of the Comptroller of the Currency finds that disclosure would compromise the safety or soundness of the financial institution or of the financial system as a whole.[94]

Some commenters specifically urged that state law enforcement be included within any delay provision,[95] and one commenter appeared to contemplate inclusion of foreign law enforcement.[96] A few commenters advocated for a confidential reporting system, whereby a registrant would initially file a nonpublic report with the Commission while a law enforcement investigation is ongoing, and then unseal the report upon the investigation's completion.[97]

A number of commenters provided feedback regarding proposed Instruction 1, which would have directed registrants to make their materiality determination regarding an incident "as

---

92 *See* letter from Hunton. This commenter also questioned whether law enforcement would be inclined to provide a written determination, particularly within four business days, because in its experience with State data breach laws, "the relevant state and federal law enforcement agencies seldom (if ever) provide written instructions when the relevant exception comes into play."

93 *See* letter from Wilson Sonsini.

94 *See* letter from BPI et al. *Cf.* letter from FSSCC.

95 *See*, *e.g.*, letter from ITIF.

96 *See* letter from CBA (stating "the scope of the contemplated exemption is indefensibly narrow, particularly for registrants with operations outside of the United States . . . there should be an exemption to permit delayed disclosure upon the request of any competent national, state or local law enforcement authority").

97 *See* letters from CSA; Hunton; SCG. *See also* letter from LTSE (positing the Regulation SCI disclosure framework as a model for Item 1.05).

soon as reasonably practicable after discovery of the incident." Several commenters recommended removing the instruction altogether as, in their view, it would place unnecessary pressure on companies to make premature determinations before they have sufficient information.[98] Other commenters stated that the instruction is too ambiguous for registrants to ascertain whether they have complied with it.[99] Conversely, one commenter advised the Commission not to provide further guidance on the meaning of "as soon as reasonably practicable," explaining that doing so would interfere with each registrant's individual assessment of what is practicable given its specific context, resulting in pressure to move more quickly than may be appropriate.[100] Another commenter likewise found that "as soon as reasonably practicable" is a "reasonable approach" that "provides public companies with the appropriate degree of flexibility to conduct a thorough assessment while ensuring that the markets get timely and relevant information."[101] One commenter recommended a safe harbor for actions and determinations made in good faith to satisfy Instruction 1 that later turn out to be mistaken.[102]

In response to a request for comment in the Proposing Release, several commenters recommended registrants be permitted to furnish rather than file an Item 1.05 Form 8-K, so that filers of an Item 1.05 Form 8-K would not be subject to liability under Section 18 of the Exchange Act.[103] A significant number of commenters also endorsed the proposal to amend 17

---

98 *See* letters from ABA; AGA/INGAA; Federated Hermes; ISA; Paylocity; Quest; SCG.

99 *See* letter from Center for Audit Quality ("CAQ"); CSA; Institute of Internal Auditors ("IIA"); LTSE; NYC Bar.

100 *See* letter from Cybersecurity Coalition.

101 *See* letter from NASAA.

102 *See* letter from Nasdaq.

103 *See* letters from BPI et al.; Business Roundtable; Chevron; CSA; EEI; LTSE; NAM; SCG.

CFR 240.13a-11(c) ("Rule 13a-11(c)") and 17 CFR 240.15d-11(c) ("Rule 15d-11(c)") under the Exchange Act to include Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or 17 CFR 240.10b-5 ("Rule 10b-5") under the Exchange Act.[104] Likewise, the proposal 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 received much support.[105]

Finally, a number of commenters averred that Item 1.05 would conflict with other Federal and state cybersecurity reporting or other regulatory regimes. For example, one commenter stated Item 1.05 would counteract the goals of CIRCIA by requiring public disclosure of information the act would keep confidential, and went on to assert that CIRCIA was intended as the primary means for reporting incidents to the Federal Government.[106] Also related to CIRCIA, a number of commenters urged harmonization of the Commission's proposal with forthcoming regulations expected from CISA pursuant to CIRCIA.[107] Several commenters alleged Item 1.05 would conflict with rules the Department of Health and Human Services ("HHS") has adopted pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") regarding the reporting of private health information breaches.[108] A few commenters likewise said Item 1.05 would conflict with the reporting regime set forth in Federal Communications Commission ("FCC") regulations for breaches of customer proprietary network

---

104 *See* letters from ABA; APCIA; BIO; Business Roundtable; Chevron; CTIA; Cybersecurity Coalition; Debevoise; EEI; LTSE; NYC Bar; PWC; SCG.

105 *See* letters from ABA; APCIA; BIO; Business Roundtable; Chevron; CTIA; Cybersecurity Coalition; Debevoise; EEI; LTSE; NYC Bar; PWC; SCG.

106 *See* letter from Sen. Portman.

107 *See* letters from ACC; ACLI; APCIA; BPI et al.; BIO; Confidentiality Coalition; Chamber; CTA; CTIA; Cybersecurity Coalition; EIC; FEI; FSSCC; Insurance Coalition ("IC"); ISA; ITI; ITIF; Nareit; NAM; NRA; R Street; SCG; SIFMA; USTelecom.

108 *See* letters from Chamber; Confidentiality Coalition; FAH; R Street.

information.[109] Conflicts were also alleged with regulations and programs of the Department of Defense ("DOD"),[110] Department of Energy ("DOE"),[111] and Department of Homeland Security ("DHS").[112] Commenters called for harmonization of Item 1.05 with regulations issued by Federal banking regulators,[113] as well as with regulations of the Federal Trade Commission ("FTC").[114] Some commenters noted the potential interaction between the proposed rules and state laws.[115] One commenter noted the McCarran-Ferguson Act, which provides that a state law preempts a Federal statute if the state law was enacted for the purpose of regulating the business of insurance and the Federal statute does not specifically relate to the business of insurance.[116]

3. Final Amendments

Having considered the comments, we remain convinced that investors need timely, standardized disclosure regarding cybersecurity incidents materially affecting registrants' businesses, and that the existing regulatory landscape is not yielding consistent and informative disclosure of cybersecurity incidents from registrants.[117] However, we are revising the proposal

---

109 *See* letters from Chamber; CTIA; USTelecom.

110 *See* letter from Chamber et al.

111 *See* letter from EEI.

112 *See* letter from ACC. This letter additionally alleged conflicts with regulations of the Department of Energy, Transportation Security Agency, Department of Defense, and Environmental Protection Agency, but did not explain specifically where those conflicts lie.

113 *See* letters from FSSCC; Structured Finance Association ("SFA"); SIFMA.

114 *See* letters from BIO; CTIA.

115 *See* letters from IC (noting "[a]n important issue will be to ensure harmonized regulation between the federal government and the several states with proposed or preexisting cybersecurity regulations"); R Street (noting that state privacy laws "mandate reporting of incidents across very different timelines"); SIFMA (noting that "many state financial services and/or insurance regulators already require regulated entities certify cybersecurity compliance").

116 *See* letter from IC.

117 As the Commission has previously stated, markets rely on timely dissemination of information to accurately and quickly value securities. *Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date*, Release No. 33-8400 (Mar. 16, 2004) [69 FR 15593 (Mar. 25, 2004)] ("Additional Form 8-K Disclosure Release"). Congress recognized that the ongoing dissemination of accurate information by issuers about

in two important respects in response to concerns raised by commenters. First, we are narrowing the amount of information required to be disclosed, to better balance investors' needs and registrants' cybersecurity posture. And second, we are providing for a delay for disclosures that would pose a substantial risk to national security or public safety, contingent on a written notification by the Attorney General, who may take into consideration other Federal or other law enforcement agencies' findings.

As described above, commenters' criticisms of Item 1.05 generally arose from two aspects of the proposal: (1) the scope of disclosure; and (2) the timing of disclosure. With respect to disclosure scope, we note in particular commenter concerns that the disclosure of certain details required by proposed Item 1.05 could exacerbate security threats, both for the registrants' systems and for systems in the same industry or beyond, and could chill threat information sharing within industries. We agree that a balancing of concerns consistent with our statutory authority is necessary in crafting Item 1.05 to avoid empowering threat actors with actionable information that could harm a registrant and its investors. However, we are not persuaded, as some commenters suggested,[118] that we should forgo requiring disclosure of the existence of an incident while it is ongoing to avoid risks, such as the risk of tipping off threat actors. Some companies already disclose material cybersecurity incidents while they are ongoing and before they are fully remediated, but the timing, form, and substance of those disclosures are inconsistent. Several commenters indicated both that investors look for information regarding registrants' cybersecurity incidents and that current disclosure levels are

---

themselves and their securities is essential to the effective operation of the markets, and specifically recognized the importance of current reporting in this regard by requiring that "[e]ach issuer reporting under Section 13(a) or 15(d) … disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer … as the Commission determines … is necessary or useful for the protection of investors and in the public interest." 15 U.S.C. 78m(l).

[118] *See supra* note 50.

inadequate to their needs in making investment decisions.[119] In addition, we note below in Section IV evidence showing that delayed reporting of cybersecurity incidents can result in mispricing of securities, and that such mispricing can be exploited by threat actors, employees, related third parties, and others through trades made before an incident becomes public.[120] Accordingly, we believe it is necessary to adopt a requirement for uniform current reporting of material cybersecurity incidents.

To that end, and to balance investors' needs with the concerns raised by commenters, we are streamlining Item 1.05 to focus the disclosure primarily on the impacts of a material cybersecurity incident, rather than on requiring details regarding the incident itself. The final rules will require the registrant to "describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations." We believe this formulation more precisely focuses the disclosure on what the company determines is the material impact of the incident, which may vary from incident to incident. The rule's inclusion of "financial condition and results of operations" is not exclusive; companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident.[121] By way of illustration, harm to a company's reputation, customer or vendor relationships, or competitiveness may be examples of a material impact on the company. Similarly, the possibility of litigation or regulatory investigations or actions, including regulatory actions by

---

[119] *See* letters from Better Markets; CalPERS; CII.

[120] *See infra* notes 413 and 462.

[121] *See also* Proposing Release at 16596 (stating that "[a] materiality analysis is not a mechanical exercise" and not solely quantitative, but rather should take into consideration "all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors").

state and Federal Governmental authorities and non-U.S. authorities, may constitute a reasonably likely material impact on the registrant.

We are not adopting, as proposed, a requirement for disclosure regarding the incident's remediation status, whether it is ongoing, and whether data were compromised. While some incidents may still necessitate, for example, discussion of data theft, asset loss, intellectual property loss, reputational damage, or business value loss, registrants will make those determinations as part of their materiality analyses. Further, we are adding an Instruction 4 to Item 1.05 to provide that a "registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." While the Commission provided this assurance in the Proposing Release,[122] we agree with some commenters that codifying it in the Item 1.05 instructions should provide added clarity to registrants on the type of disclosure required by Item 1.05.

With respect to commenters' questions concerning the application of Item 1.05 to incidents occurring on third-party systems, we are not exempting registrants from providing disclosures regarding cybersecurity incidents on third-party systems they use, nor are we providing a safe harbor for information disclosed about third-party systems. While we appreciate the commenters' concerns about a registrant's reduced control over such systems, we note the centrality of the materiality determination: whether an incident is material is not contingent on where the relevant electronic systems reside or who owns them. In other words, we do not believe a reasonable investor would view a significant breach of a registrant's data as immaterial merely because the data were housed on a third-party system, especially as

[122] *Id*. at 16595.

companies increasingly rely on third-party cloud services that may place their data out of their immediate control.[123] Instead, as discussed above, materiality turns on how a reasonable investor would consider the incident's impact on the registrant.

Depending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and the customer, or by one but not the other, or by neither. We appreciate that companies may have reduced visibility into third-party systems; registrants should disclose based on the information available to them. The final rules generally do not require that registrants conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with registrants' disclosure controls and procedures. This is consistent with the Commission's general rules regarding the disclosure of information that is difficult to obtain.[124]

Turning to disclosure timing, we believe that the modifications from the proposed rules regarding the disclosures called for by Item 1.05 alleviate many of the concerns some commenters had regarding the proposed disclosure deadline of four business days from the materiality determination. Because the streamlined disclosure requirements we are adopting are focused on an incident's basic identifying details and its material impact or reasonably likely material impact, the registrant should have the information required to be disclosed under this rule as part of conducting the materiality determination. For example, most organizations' materiality analyses will include consideration of the financial impact of a cybersecurity

---

123 *See* Deloitte, *Global Third-Party Risk Management Survey 2022*, at 15, *available at* h*ttps://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-global-tprm-survey-report-2022.pdf* (discussing results of a global survey of 1,309 "senior leaders from a variety of organizations" indicating that "73% of respondents currently have a moderate to high level of dependence on [cloud-service providers]" and "[t]hat is expected to increase to 88% in the years ahead").

124 *See* 17 CFR 230.409 and 17 CFR 240.12b-21, which provide that information need only be disclosed insofar as it is known or reasonably available to the registrant. Accordingly, we are not providing additional time to comply with Item 1.05 as it relates to third-party incidents, as requested by some commenters.

incident, so information regarding the incident's impact on the registrant's financial condition and results of operations will likely have already been developed when Item 1.05 is triggered.[125] Thus, we believe that the four business day timeframe from the date of a materiality determination will be workable.

The reformulation of Item 1.05 also addresses the concern among commenters that the disclosure may be tentative and unclear, resulting in false positives and mispricing in the market. In the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered. The registrant will develop information after discovery until it is sufficient to facilitate a materiality analysis.[126] At that point, we believe investors are best served knowing, within four business days after the materiality determination, that the incident occurred and what led management to conclude the incident is material. While it is possible that occasionally there may be incidents that initially appear material but developments after the filing of the Item 1.05 Form 8-K reveal to be not material, the alternative of delaying disclosure beyond the four business day period after a materiality determination has the potential to lead to far more mispricing and will negatively impact investors making investment and voting decisions without the benefit of knowing that there is a material cybersecurity incident.

Commenters posited an array of alternative deadlines for the Item 1.05 Form 8-K, as recounted above. We are not persuaded by commenters' arguments that disclosure should be delayed until companies mitigate, contain, remediate, or otherwise diminish the harm of the incident, because, as discussed above, Item 1.05 does not require disclosure of the types of

---

[125] To the extent any required information is not determined or is unavailable at the time of the required filing, Instruction 2 to Item 1.05, as adopted, directs the registrant to include a statement to this effect in the Form 8-K and then file a Form 8-K amendment containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available. *See infra* Section II.B.3.

[126] As discussed below, registrants should develop such information without unreasonable delay.

details that have the potential to be exploited by threat actors, but rather focuses on the incident's material impact or reasonably likely material impact on the registrant. While there may be, as commenters noted, some residual risk of the disclosure of an incident's existence tipping off threat actors, such risk is justified, in our view, by investors' need for timely information, and similar risk already exists today with some companies' current cybersecurity incident disclosure practices. We are also not persuaded that Item 1.05 is sufficiently different from other Form 8-K items such that deviating from the form's four business day deadline following the relevant trigger would be indicated. While some commenters argued that Item 1.05 is qualitatively different from all other Form 8-K filings in that its trigger is largely outside the company's control, we disagree because other Form 8-K items may also be triggered unexpectedly, such as Item 4.01 (Changes in Registrant's Certifying Accountants) and Item 5.02 (Departure of Directors or Principal Officers). And as compared to those items, the information needed for Item 1.05 may be further along in development when the filing is triggered, whereas, for example, a company may have no advance warning that a principal officer is departing.

With respect to the five business day deadline suggested by a few commenters to allow registrants a full calendar week from the materiality determination to the disclosure, we note that in the majority of cases registrants will have had additional time leading up to the materiality determination, such that disclosure becoming due less than a week after discovery should be uncommon. More generally with respect to the various alternative timing suggestions, we observe that the Commission adopted the uniform four business day deadline in 2004 to simplify the previous bifurcated deadlines, and we find commenters have not offered any compelling

rationale to return to bifurcated deadlines.[127] Form 8-K provides for current reporting of events that tend to be material to investor decision-making, and we see no reason to render the reporting of Item 1.05 less current than other Form 8-K items.

In the Proposing Release, the Commission requested comment on whether to allow registrants to delay filing an Item 1.05 Form 8-K where the Attorney General determines that a delay is in the interest of national security.[128] In response to comments, we are adopting a delay provision in cases where disclosure poses a substantial risk to national security or public safety. Pursuant to Item 1.05(c), a registrant may delay making an Item 1.05 Form 8-K filing if the Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the Commission of such determination in writing.[129] Initially, disclosure may be delayed for a time period specified by the Attorney General, up to 30 days following the date when the disclosure was otherwise required to be provided. The delay may be extended for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing.

In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. We are

---

127 *See* Additional Form 8-K Disclosure Release. *See also Proposed Rule: Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date*, Release No. 33-8106 (June 17, 2002) [67 FR 42914 (June 25, 2002)].

128 Proposing Release at 16598.

129 We note that the delay provision we are adopting does not relieve a company's obligations under Regulation FD or with respect to the securities laws' antifraud prohibitions that proscribe certain insider trading, including Exchange Act Section 10(b). Under Regulation FD, material nonpublic information disclosed to any investor, for example, through investor outreach activities, would be required to be disclosed publicly, subject to limited exceptions. *See* 17 CFR 243.100 *et seq.*

providing for the final additional delay period in recognition that, in extraordinary circumstances, national security concerns may justify additional delay beyond that warranted by public safety concerns, due to the relatively more critical nature of national security concerns. Beyond the final 60-day delay, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order.[130]

We have consulted with the Department of Justice to establish an interagency communication process to allow for the Attorney General's determination to be communicated to the Commission in a timely manner. The Department of Justice will notify the affected registrant that communication to the Commission has been made, so that the registrant may delay filing its Form 8-K.

We agree with commenters that a delay is appropriate for the limited instances in which public disclosure of a cybersecurity incident may cause harm to national security or public safety. The final rules appropriately balance such security concerns against investors' informational needs. In particular, the provision's "substantial risk to national security or public safety" bases are sufficiently expansive to ensure that significant risks of harm from disclosure may be protected against, while also ensuring that investors are not denied timely access to material information.[131] With respect to commenters who recommended that other Federal

---

[130] Any exercise of exemptive authority in these circumstances would need to meet all of the standards of Section 36 of the Exchange Act. Furthermore, Item 1.05 of Form 8-K in no way limits the Commission's general exemptive authority under Section 36.

[131] The delay provision for substantial risk to national security or public safety is separate from Exchange Act Rule 0-6, which provides for the omission of information that has been classified by an appropriate department or agency of the Federal Government for the protection of the interest of national defense or foreign policy. If the information a registrant would otherwise disclose on an Item 1.05 Form 8-K or pursuant to Item 106 of Regulation S-K or Item 16K of Form 20-F is classified, the registrant should comply with Exchange Act Rule 0-6.

agencies and non-Federal law enforcement agencies also be permitted to trigger a delay or who argued that other agencies may be the primary organization in the Federal Government for the response, we note that the rule does not preclude any such agency from requesting that the Attorney General determine that the disclosure poses a substantial risk to national security or public safety and communicate that determination to the Commission. However, we believe that designating a single law enforcement agency as the Commission's point of contact on such delays is critical to ensuring that the rule is administrable.

Turning to other timing-related issues raised by commenters, we are not adopting commenters' suggestion to replace Item 1.05 with periodic reporting of material cybersecurity incidents on Forms 10-Q and 10-K because such an approach may result in significant variance as to when investors learn of material cybersecurity incidents. Based on when an incident occurs during a company's reporting cycle, the timing between the materiality determination and reporting on the next Form 10-Q or Form 10-K could vary from a matter of months to a matter of weeks or less. For example, if two companies experience a similar cybersecurity incident, but one determines the incident is material early during a quarterly period and the other makes such determination at the end of the quarterly period, commenters' suggested approach would have both companies report the incident around the same time despite the first company having determined the incident was material weeks or months sooner, which would result in a significant delay in this information being provided to investors. Such variance would therefore reduce comparability across registrants and may put certain registrants at a competitive disadvantage.

We also decline to use a quantifiable trigger for Item 1.05 because some cybersecurity incidents may be material yet not cross a particular financial threshold. We note above that the

material impact of an incident may encompass a range of harms, some quantitative and others qualitative. A lack of quantifiable harm does not necessarily mean an incident is not material. For example, an incident that results in significant reputational harm to a registrant may not be readily quantifiable and therefore may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material. Similarly, whereas a cybersecurity incident that results in the theft of information may not be deemed material based on quantitative financial measures alone, it may in fact be material given the impact to the registrant that results from the scope or nature of harm to individuals, customers, or others, and therefore may need to be disclosed.

In another change from the proposal, and to respond to commenters' concerns that the proposed "as soon as reasonably practicable" language in Instruction 1 could pressure companies to draw conclusions about incidents with insufficient information, we are revising the instruction to state that companies must make their materiality determinations "without unreasonable delay." As explained in the Proposing Release, the instruction was intended to address any concern that some registrants may delay making such a determination to avoid a disclosure obligation.[132] We understand commenter concerns that the proposed instruction could result in undue pressure to make a materiality determination before a registrant has sufficient information to do so, and we recognize that a materiality determination necessitates an informed and deliberative process. We believe the revised language should alleviate this unintended consequence, while providing registrants notice that, though the determination need not be rushed prematurely, it also cannot be unreasonably delayed in an effort to avoid timely disclosure. For example, for incidents that

[132] Proposing Release at 16596.

impact key systems and information, such as those the company considers its "crown jewels,"[133] as well as incidents involving unauthorized access to or exfiltration of large quantities of particularly important data, a company may not have complete information about the incident but may know enough about the incident to determine whether the incident was material. In other words, a company being unable to determine the full extent of an incident because of the nature of the incident or the company's systems, or otherwise the need for continued investigation regarding the incident, should not delay the company from determining materiality. Similarly, if the materiality determination is to be made by a board committee, intentionally deferring the committee's meeting on the materiality determination past the normal time it takes to convene its members would constitute unreasonable delay.[134] As another example, if a company were to revise existing incident response policies and procedures in order to support a delayed materiality determination for or delayed disclosure of an ongoing cybersecurity event, such as by extending the incident severity assessment deadlines, changing the criteria that would require reporting an incident to management or committees with responsibility for public disclosures, or introducing other steps to delay the determination or disclosure, that would constitute unreasonable delay. In light of the revision to Instruction 1, we find that a safe harbor, as suggested by some commenters, is unnecessary; adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance. Importantly, we remind registrants, as the Commission did in the Proposing Release, that

---

133 *See* National Cybersecurity Alliance, *Identify Your "Crown Jewels"* (July 1, 2022), *available at https://staysafeonline.org/cybersecurity-for-business/identify-your-crown-jewels/* (explaining that "[c]rown jewels are the data without which your business would have difficulty operating and/or the information that could be a high-value target for cybercriminals").

134 We note that Form 8-K Item 1.05 does not specify whether the materiality determination should be performed by the board, a board committee, or one or more officers. The company may establish a policy tasking one or more persons to make the materiality determination. Companies should seek to provide those tasked with the materiality determination information sufficient to make disclosure decisions.

"[d]oubts as to the critical nature" of the relevant information "will be commonplace" and should "be resolved in favor of those the statute is designed to protect," namely investors.[135]

Revised Instruction 1 should also reassure registrants that they should continue sharing information with other companies or government actors about emerging threats. Such information sharing may not necessarily result in an Item 1.05 disclosure obligation. The obligation to file the Item 1.05 disclosure is triggered once a company has developed information regarding an incident sufficient to make a materiality determination, and a decision to share information with other companies or government actors does not in itself necessarily constitute a determination of materiality. A registrant may alert similarly situated companies as well as government actors immediately after discovering an incident and before determining materiality, so long as it does not unreasonably delay its internal processes for determining materiality.

As proposed, we are adding Item 1.05 to the list of Form 8-K items in General Instruction I.A.3.(b) of Form S-3 , so that the untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility.[136] We note the significant support from commenters regarding this proposal, and as noted in the Proposing Release, continue to believe that the consequences of the loss of Form S-3 eligibility would be unduly severe given the circumstances that will surround Item 1.05 disclosures. Likewise, as supported by many commenters, we are adopting as proposed amendments to 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. This accords with the view the

---

[135] Proposing Release at 16596 (quoting *TSC Indus. v. Northway*, 426 U.S. at 448). The Court's opinion in *TSC Indus.* has a nuanced discussion of the balance of considerations in setting a materiality standard. 426 U.S. at 448-450.

[136] Because of our decision to exempt asset-backed issuers from the new rules (*see infra* Section II.G.1), we are not amending Form SF-3.

Commission articulated in 2004 that the safe harbor is appropriate if the triggering event for the Form 8-K requires management to make a rapid materiality determination.[137]

We decline to permit registrants to furnish rather than file the Item 1.05 Form 8-K, as suggested by some commenters. While we understand commenters' points that reducing liability may ease the burden on registrants, we believe that treating Item 1.05 disclosures as filed will help promote the accuracy and reliability of such disclosures for the benefit of investors. Of the existing Form 8-K items, only Items 2.02 (Results of Operations and Financial Condition) and 7.01 (Regulation FD Disclosure) are permitted to be furnished rather than filed. The Commission created exceptions for those two items to allay concerns that do not pertain here. Specifically, with respect to Item 2.02, the Commission was motivated by concerns that requiring the information to be filed would discourage registrants from proactively issuing earnings releases and similar disclosures.[138] Similarly, with respect to Item 7.01, the Commission decided to allow the disclosure to be furnished to address concerns that, if required to be filed, the disclosure could be construed as an admission of materiality, which might lead some registrants to avoid making proactive disclosure.[139] By contrast, Item 1.05 is not a voluntary disclosure, and it is by definition material because it is not triggered until the registrant determines the materiality of an incident. It is thus more akin to the Form 8-K items other than Items 2.02 and 7.01, in that it is a description of a material event that has occurred about which investors need adequate information. Therefore, the final rules require an Item 1.05 Form 8-K to be filed.

---

137 Additional Form 8-K Disclosure Release at 15607.

138 *See Conditions for Use of Non-GAAP Financial Measures*, Release No. 33-8176 (Jan. 22, 2003) [68 FR 4819 (Jan. 30, 2003)].

139 *See Selective Disclosure and Insider Trading*, Release No. 33-7881 (Aug. 15, 2000) [65 FR 51715 (Aug. 24, 2000)].

We are not including a new rule to ban trading by insiders during the materiality determination time period, as suggested by some commenters. Those with a fiduciary duty or other relationship of trust and confidence are already prohibited from trading while in possession of material, nonpublic information.[140] And because we are adopting the four business days from materiality determination deadline, we agree with the point raised by some commenters that the risk of insider trading is low given the limited time period between experiencing a material incident and public disclosure. We also note that we recently adopted amendments to 17 CFR 240.10b5-1 ("Rule 10b5-1") that added a certification condition for directors and officers wishing to avail themselves of the rule's affirmative defense; specifically, if relying on the amended affirmative defense, directors and officers need to certify in writing, at the time they adopt the trading plan, that they are unaware of material nonpublic information about the issuer or its securities, and are adopting the plan in good faith and not as part of a plan or scheme to evade the insider trading prohibitions.[141] Therefore, given the timing of the incident disclosure requirement as well as the recently adopted amendments to Rule 10b5-1, we do not find need for a new rule banning trading by insiders during the time period between the materiality determination and disclosure.

A number of commenters raised concerns about conflicts with other Federal laws and regulations. Of the Federal laws and regulations that we reviewed and commenters raised concerns with, we have identified one conflict, with the FCC's notification rule for breaches of

[140] *United States v. O'Hagan*, 521 U.S. 642 (1997).

[141] *See Insider Trading Arrangements and Related Disclosures*, Release No. 33-11138 (Dec. 14, 2022) [87 FR 80362 (Dec. 29, 2022)].

customer proprietary network information ("CPNI").[142] Of the remaining Federal laws and regulations noted by commenters as presenting conflicts, our view is that Item 1.05 neither directly conflicts with nor impedes the purposes of other such laws and regulations.

The FCC's rule for notification in the event of breaches of CPNI requires covered entities to notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") no later than seven business days after reasonable determination of a CPNI breach, and further directs the entities to refrain from notifying customers or disclosing the breach publicly until seven business days have passed following the notification to the USSS and FBI.[143] To accommodate registrants who are subject to this rule and may as a result face conflicting disclosure timelines,[144] we are adding paragraph (d) to Item 1.05 providing that such registrants may delay making a Form 8-K disclosure up to the seven business day period following notification to the USSS and FBI specified in the FCC rule, [145] with written notification to the Commission.[146]

---

142 47 CFR 64.2011. CPNI is defined in 47 CFR 222(h)(1) as: "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information."

143 We note that the FCC recently proposed amending its rule; among other things, the proposal would eliminate the seven-business day waiting period, potentially eliminating the conflict. Federal Communications Commission, *Data Breach Reporting Requirements*, 88 FR 3953 (Jan. 23, 2023).

144 Commission staff consulted with FCC staff about a potential delay provision to address any conflict between the FCC rule and the Form 8-K reporting requirements.

145 The exception we are creating does not apply to 47 CFR 64.2011(b)(3), which provides that the USSS or FBI may direct the entity to further delay notification to customers or public disclosure beyond seven business days if such disclosure "would impede or compromise an ongoing or potential criminal investigation or national security." If the USSS or FBI believes that disclosure would result in a substantial risk to national security or public safety, it may, as explained above, work with the Department of Justice to seek a delay of disclosure.

146 Such notice should be provided through correspondence on EDGAR no later than the date when the disclosure required by Item 1.05 was otherwise required to be provided.

We also considered the conflicts commenters alleged with CIRCIA. Specifically, they stated that Item 1.05 is at odds with the goals of CIRCIA, and that it may conflict with forthcoming regulations from CISA. The confidential reporting system established by CIRCIA serves a different purpose from Item 1.05 and through different means; the former focuses on facilitating the Federal Government's preparation for and rapid response to cybersecurity threats, while the latter focuses on providing material information about public companies to investors in a timely manner. While CISA has yet to propose regulations to implement CIRCIA, given the statutory authority, text, and legislative history of CIRCIA, it appears unlikely the regulations would affect the balance of material information available to investors about public companies, because the reporting regime CIRCIA establishes is confidential.[147] Nonetheless, the Commission participates in interagency working groups on cybersecurity regulatory implementation, and will continue to monitor developments in this area to determine if modification to Item 1.05 becomes appropriate in light of future developments.[148]

We also considered the HIPAA-related conflict alleged by commenters, specifically with respect to HHS's rule on Notification in the Case of Breach of Unsecured Protected Health Information. That rule provides, in the event of a breach of unsecured protected health information, for the covered entity to provide notification to affected individuals "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."[149] If the breach involves more than 500 residents of a state or jurisdiction, the rule directs the covered

---

147 6 U.S.C. 681e.

148 Should a conflict arise in the future with CISA regulations or regulations of another Federal agency, the Commission can address such conflict via rulemaking or other action at that time.

149 45 CFR 164.404(b). The notification must describe the breach, the types of unsecured protected health information involved, steps the individuals should take to protect themselves, what the entity is doing to mitigate harm and remediate, and where the individuals can seek additional information. *Id.*

entity to also notify prominent media outlets within the same timeframe.[150] The rule further provides that if a company receives written notice from "a law enforcement official" requesting a delay and specifying the length of the delay, then the company "shall … delay such notification, notice, or posting for the time period specified by the official."[151]

We do not view Form 8-K Item 1.05 as implicated by the HHS rule. Importantly, the HHS rule's delay provision applies specifically to any "notification, notice, or posting required under this subpart," or in other words notice to affected individuals, media, and the Secretary of HHS.[152] Such notification focuses on the consequences of the breach for the affected individuals; for example, individuals must be told what types of protected health information were accessed, and what steps they should take to protect themselves from harm.[153] This is different from the disclosure required by Item 1.05, which focuses on the consequences for the company that are material to investors, and whose timing is tied not to discovery but to a materiality determination. The HHS rule does not expressly preclude the latter type of public disclosure, or other potential communications companies experiencing a breach may make. Therefore, we believe that a registrant subject to the HHS rule will not face a conflict in complying with Item 1.05.[154]

We also considered the conflicts commenters alleged with regulations and programs of DOD, DOE, DHS, the Federal banking regulatory agencies, state insurance laws, and miscellaneous other Federal agencies or laws. We find that, while there may be some overlap of

---

150 45 CFR 164.406.

151 45 CFR 164.412.

152 *Id.*

153 45 CFR 164.404(c).

154 For the same reason, the Federal Trade Commission's Health Breach Notification rule, which is similar to HHS's rule, does not present a conflict either. *See* 16 CFR part 318.

subject matter, Item 1.05 neither conflicts with nor impedes the purpose of those regulations and programs.[155] We disagree with one commenter's assertion that cybersecurity incident disclosure "falls squarely within the jurisdiction of state insurance commissioners" as state cybersecurity incident reporting regulations would not pertain to the "business of insurance" as courts have interpreted the McCarran-Ferguson Act, and the commenter did not note any particular state insurance laws that would present a conflict.[156] With respect to Federal banking regulatory agencies specifically, we note that, in the event they believe that the disclosure of a material cybersecurity incident would threaten the health of the financial system in such a way that results in a substantial risk to national security or public safety, they may, as explained above, work with the Department of Justice to seek to delay disclosure.

It would not be practical to further harmonize Item 1.05 with other agencies' cybersecurity incident reporting regulations, as one commenter suggested,[157] because Item 1.05 serves a different purpose—it is focused on the needs of investors, rather than the needs of regulatory agencies, affected individuals, or the like. With respect to state insurance and privacy laws, commenters did not provide any evidence sufficient to alter the Commission's finding in the Proposing Release that, to the extent that Item 1.05 would require disclosure in a situation where state law would excuse or delay notification, we consider prompt reporting of material cybersecurity incidents to investors critical to investor protection and well-functioning, orderly, and efficient markets.

---

155 For example, one commenter alleged conflicts with DHS's Chemical Facilities Anti-Terrorism Standards program ("CFATS") and with the Maritime Transportation Security Act ("MTSA"). *See* letter from American Chemistry Council. Both CFATS and MTSA provide for the protection of certain sensitive information, but neither is implicated by cybersecurity incident disclosure to the Commission.

156 *See, e.g., SEC v. National Sec., Inc.*, 393 U.S. 453 (1969).

157 *See* letter from BIO.

B. Disclosures about Cybersecurity Incidents in Periodic Reports

1. Proposed Amendments

The Commission proposed to add new Item 106 to Regulation S-K to, among other things, require updated cybersecurity disclosure in periodic reports. If a registrant previously provided disclosure regarding one or more cybersecurity incidents pursuant to Item 1.05 of Form 8-K, proposed 17 CFR 229.106(d)(1) (Regulation S-K "Item 106(d)(1)") would require such registrant to disclose "any material changes, additions, or updates" on the registrant's quarterly report on Form 10-Q or annual report on Form 10-K.[158] In addition, proposed Item 106(d)(1) would require disclosure of the following information:

- Any material effect of the incident on the registrant's operations and financial condition;
- Any potential material future impacts on the registrant's operations and financial condition;
- Whether the registrant has remediated or is currently remediating the incident; and
- Any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.[159]

The Commission explained that it paired current reporting under Item 1.05 of Form 8-K with periodic reporting under 17 CFR 229.106(d) (Regulation S-K "Item 106(d)") to balance investors' need for timely disclosure with their need for complete disclosure.[160] When an Item 1.05 Form 8-K becomes due, the Commission noted, a registrant may not possess complete

---

158 Proposing Release at 16598.

159 *Id*.

160 *Id.*

information about the material cybersecurity incident. Accordingly, under the proposed rules, a registrant would provide the information known at the time of the Form 8-K filing and follow up in its periodic reports with more complete information as it becomes available, along with any updates to previously disclosed information.

The Commission also proposed 17 CFR 229.106(d)(2) (Regulation S-K "Item 106(d)(2)") to require disclosure in a registrant's next periodic report when, to the extent known to management, a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate.[161] The Proposing Release explained that this requirement may be triggered where, for example, a threat actor engages in a number of smaller but continuous related cyberattacks against the same company and collectively they become material.[162] Item 106(d)(2) would require disclosure of essentially the same information required in proposed Item 1.05 of Form 8-K, as follows:

- A general description of when the incidents were discovered and whether they are ongoing;
- A brief description of the nature and scope of the incidents;
- Whether any data were stolen or altered in connection with the incidents;
- The effect of the incidents on the registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incidents.[163]

[161] *Id.* at 16599.

[162] *Id.*

[163] *Id.* at 16619-16620.

2. Comments

Reaction among commenters to proposed Item 106(d)(1) was mixed. Some wrote in support, noting that updated incident disclosure is needed to avoid previously disclosed information becoming stale and misleading as more information becomes available, and saying that updates help investors assess the efficacy of companies' cybersecurity procedures.[164] Others took issue with specific aspects of the proposed rule. For example, some commenters stated that the proposed requirement to disclose "any potential material future impacts" is vague and difficult to apply, and urged removing or revising it.[165] Similarly, other commenters said that registrants should not be required to describe progress on remediation, noting that such information could open them up to more attacks.[166] In the same vein, one commenter suggested that no updates be required until remediation is sufficiently complete.[167] One commenter said the requirement to disclose changes in policies and procedures is unnecessary and overly broad,[168] and another commenter said the requirement should be narrowed to "material changes."[169]

More generally, commenters sought clarification on how to differentiate instances where updates should be included in periodic reports from instances where updates should be filed on Form 8-K; they found the guidance in the Proposing Release on this point "unclear."[170] And one

---

164 *See* letters from AICPA; Crindata; R Street. *See also* IAC Recommendation.

165 *See* letters from EEI; Prof. Perullo; PWC; SCG.

166 *See* letters from BCE; BPI et al.; Enbridge. *See also* letter from EEI (suggesting narrowing the rule to "material remediation," and delaying such disclosure until remediation is complete).

167 *See* letter from EEI.

168 *See* letter from Prof. Perullo.

169 *See* letter from EEI.

170 *See* letter from PWC; *accord* letter from Deloitte. The Proposing Release stated: "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." Proposing Release at 16598.

commenter argued that, regardless of where the update is filed, the incremental availability of information would make it difficult for companies to determine when the update requirement is triggered.[171]

With respect to proposed Item 106(d)(2), a large number of commenters expressed concern about the aggregation requirement, saying, for example, that companies experience too many events to realistically communicate internally upward to senior management, and that retaining and analyzing data on past events would be too costly.[172] A number of other commenters relatedly said that, for the aggregation requirement to be workable, companies need more guidance on the nature, timeframe, and breadth of incidents that should be collated.[173] In this regard, one supporter of the requirement explained in its request for additional guidance that "cybersecurity incidents are so unfortunately common that a strict reading of this section could cause overreporting to the point that it is meaningless for shareholders."[174]

Some commenters suggested revising the rule to cover only "related" incidents.[175] Possible definitions offered for "related" incidents included those "performed by the same malicious actor or that exploited the same vulnerability,"[176] and those resulting from "attacks on the same systems, processes or controls of a registrant over a specified period of time."[177] Suggestions for limiting the time period over which aggregation should occur included the

---

171 *See* letter from Quest.

172 *See* letters from ABA; ACLI; AIA; Business Roundtable; EEI; Enbridge; Ernst & Young LLP ("E&Y"); FAH; FedEx; Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies ("FDD"); GPA; Hunton; ITI; ISA; LTSE; Microsoft; Nareit; NAM; NDIA; NRA; Prof. Perullo; SCG; SIFMA.

173 *See* letters from ACC; APCIA; BDO USA, LLP ("BDO"); BPI et al.; CAQ; Chamber; Chevron; Deloitte; EIC; FEI; M. Barragan; PWC; R Street.; TransUnion.

174 *See* letter from R Street.

175 *See* letters from ABA; APCIA; EEI; E&Y; PWC.

176 *See* letter from ABA.

177 *See* letter from E&Y.

preceding one year,[178] and the preceding two years.[179] One commenter requested the Commission clarify that a company's Item 106(d)(2) disclosure need describe only the aggregate material impact of the incidents, rather than describing each incident individually; the commenter was concerned with threat actors becoming informed of a company's vulnerabilities through overly detailed disclosure.[180] Another commenter suggested granting registrants additional time to come into compliance with Item 106(d)(2) after Commission adoption, so that they can develop system functionality to retain details about immaterial incidents.[181]

Commenters also wrote in support of the aggregation requirement.[182] One of these commenters stated that aggregation is needed especially where an advanced persistent threat actor[183] seeks to exfiltrate data or intellectual property over time.[184]

3. Final Amendments

In response to comments, we are not adopting proposed Item 106(d)(1) and instead are adopting a new instruction to clarify that updated incident disclosure must be provided in a Form 8-K amendment. Specifically, we are revising proposed Instruction 2 to Item 1.05 of Form 8-K to direct the registrant to include in its Item 1.05 Form 8-K a statement identifying any

---

178 *See* letter from APCIA.

179 *See* letter from EEI.

180 *See* letter from AGA/INGAA.

181 *See* letter from Deloitte.

182 *See* letters from CII; CSA; R Street; NASAA.

183 The National Institute of Standards and Technology explains that an advanced persistent threat "is an adversary or adversarial group that possesses the expertise and resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. The APT objectives include establishing a foothold within the infrastructure of targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, function, program, or organization; or positioning itself to carry out these objectives in the future. The APT pursues its objectives repeatedly over an extended period, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives." National Institute of Standards and Technology, *NIST Special Publication 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information* (Feb. 2021), at 2.

184 *See* letter from CSA.

information called for in Item 1.05(a) that is not determined or is unavailable at the time of the required filing and then file an amendment to its Form 8-K containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available. This change mitigates commenters' concerns with Item 106(d)(1). In particular, under the final rules, companies will not have to distinguish whether information regarding a material cybersecurity incident that was not determined or was unavailable at the time of the initial Form 8-K filing should be included on current reports or periodic reports, as the reporting would be in an amended Form 8-K; details that commenters suggested raised security concerns, such as remediation status, are not required; and concerns that the proposed rule was vague or overbroad have been addressed by narrowing the required disclosure to the information required by Item 1.05(a). We also believe that use of a Form 8-K amendment rather than a periodic report will allow investors to more quickly identify updates regarding incidents that previously were disclosed.

We appreciate that new information on a reported cybersecurity incident may surface only in pieces; the final rules, however, do not require updated reporting for *all* new information. Rather, Instruction 2 to Item 1.05 directs companies to file an amended Form 8-K with respect to any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing. Other than with respect to such previously undetermined or unavailable information, the final rules do not separately create or otherwise affect a registrant's duty to update its prior statements. We remind registrants, however, that they may have a duty to correct prior disclosure that the registrant determines was untrue (or omitted a material fact

necessary to make the disclosure not misleading) at the time it was made[185] (for example, if the registrant subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made[186] (for example, when the original statement is still being relied on by reasonable investors). Registrants should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.[187]

We are not adopting proposed Item 106(d)(2), in response to concerns that the proposed aggregation requirement was vague or difficult to apply. We are persuaded by commenters that the proposed requirement might be difficult to differentiate from Item 1.05 disclosure, or by contrast, could result in the need for extensive internal controls and procedures to monitor all immaterial events to determine whether they have become collectively material. The intent of the proposed requirement was to capture the material impacts of related incidents, and prevent the avoidance of incident disclosure through disaggregation of such related events. However, upon further reflection, and after review of comments, we believe that the proposed requirement is not necessary based on the scope of Item 1.05.

To that end, we emphasize that the term "cybersecurity incident" as used in the final rules is to be construed broadly, as the Commission stated in the Proposing Release.[188] The definition

---

185 *See Backman v. Polaroid Corp.*, 910 F.2d 10, 16-17 (1st Cir. 1990) (en banc) (finding that the duty to correct applies "if a disclosure is in fact misleading when made, and the speaker thereafter learns of this").

186 *See id*. at 17 (describing the duty to update as potentially applying "if a prior disclosure 'becomes materially misleading in light of subsequent events'" (quoting *Greenfield v. Heublein, Inc.*, 742 F.2d 751, 758 (3d Cir. 1984))). *But see Higginbotham v. Baxter Intern., Inc.*, 495 F.3d 753, 760 (7th Cir. 2007) (rejecting duty to update before next quarterly report); *Gallagher v. Abbott Laboratories*, 269 F.3d 806, 808-11 (7th Cir. 2001) (explaining that securities laws do not require continuous disclosure).

187 Relatedly, registrants should be aware of the requirement under Item 106(b)(2) of Regulation S-K to describe "[w]hether any risks from cybersecurity threats, *including as a result of any previous cybersecurity incidents*, have materially affected or are reasonably likely to materially affect the registrant" (emphasis added). *See infra* Section II.C.1.c.

188 Proposing Release at 16601.

of "cybersecurity incident" we are adopting extends to "a series of related unauthorized occurrences."[189] This reflects that cyberattacks sometimes compound over time, rather than present as a discrete event. Accordingly, when a company finds that it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each by itself immaterial. One example was provided in the Proposing Release: the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material.[190] Another example is a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially.

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

1. Risk Management and Strategy

a. Proposed Amendments

The Commission proposed to add 17 CFR 229.106(b) (Regulation S-K "Item 106(b)") to require registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy in their annual reports. The Commission noted the Division of Corporation Finance staff's experience that most registrants disclosing a cybersecurity incident do not describe their cybersecurity risk oversight or any related policies and procedures, even though companies typically address significant risks by developing risk

[189] *See infra* Section II.C.3.

[190] Proposing Release at 16599.

management systems that often include written policies and procedures.[191]

Proposed Item 106(b) would require a description of the registrant's policies and procedures, if any, for the identification and management of 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. As proposed, registrants would be required to include a discussion, as applicable, of:

- Whether the registrant has a cybersecurity risk assessment program and if so, a description of the program ((b)(1));
- Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program ((b)(2));
- Whether the registrant has policies and procedures to oversee, identify, and mitigate 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 ((b)(3));
- Whether the registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents ((b)(4));
- Whether the registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident ((b)(5));

[191] *Id*.

- Whether previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies ((b)(6));
- Whether 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 ((b)(7)); and
- Whether cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation and if so, how ((b)(8)).[192]

The Commission anticipated that proposed Item 106(b) would benefit investors by requiring more consistent disclosure of registrants' strategies and actions to manage cybersecurity risks.[193] Such risks, the Commission observed, can affect registrants' business strategy, financial outlook, and financial planning, as companies increasingly rely on information technology, collection of data, and use of digital payments as critical components of their businesses.[194]

The Commission noted that the significant number of cybersecurity incidents pertaining to third-party service providers prompted the proposal to require disclosure of registrants' selection and oversight of third-party entities.[195] The Commission also proposed requiring discussion of how prior cybersecurity incidents have affected or are reasonably likely to affect the registrant, because such disclosure would equip investors to better comprehend the level of cybersecurity risk the company faces and assess the company's preparedness regarding such

---

[192] *Id.* at 16599-16600.

[193] *Id.* at 16599.

[194] *Id.*

[195] *Id.*

risk.[196]

b. Comments

Many commenters supported proposed Item 106(b) for requiring information that is vital to investors as they assess companies' risk profiles and make investment decisions.[197] One said cybersecurity disclosures now are "scattered and unpredictable" rather than "uniform," which "diminishes their effectiveness."[198] Similarly, another found that current disclosures "do not provide investors with the information necessary to evaluate whether companies have adequate governance structures and measures in place to deal with cybersecurity challenges."[199] The IAC recommended extending the proposed Item 106(b) disclosure requirements (as well as the proposed Item 106(c) disclosure requirements) to registration statements, stating that "pre-IPO companies may face heightened [cybersecurity] risks."[200]

By contrast, a number of commenters opposed proposed Item 106(b). In particular, they commented that much of the proposed Item 106(b) disclosure could increase a company's vulnerability to cyberattacks; they expressed particular concern regarding the potential harms from disclosures about whether cybersecurity policies are in place, incident response processes and techniques, previous incidents and what changes they spurred, and third-party service providers.[201] Another criticism was that proposed Item 106(b) would effectively force companies

---

196 *Id.*

197 *See* letters of AICPA; BuildingCyberSecurity.org ("BCS"); Better Markets; Bitsight; Blue Lava, Inc. ("Blue Lava"); CalPERS; ITIF; National Association of Corporate Directors ("NACD"); NASAA; PWC; PRI; R Street; SecurityScorecard; Tenable Holdings Inc. ("Tenable"). *See also* IAC Recommendation.

198 *See* letter from Better Markets.

199 *See* letter from PRI.

200 *See* IAC Recommendation.

201 *See* letters from ABA; ACLI; APCIA; BIO; BPI et al.; Business Roundtable; Chamber; CSA; CTIA; EIC; Enbridge; FAH; Federated Hermes; GPA; ITI; ISA; Nareit; NAM; NMHC; NRA; National Retail Federation ("NRF"); SIFMA; Sen. Portman; TechNet; TransUnion; USTelecom; Virtu.

to model their cybersecurity policies on the rule's disclosure elements, rather than the practices best suited to each company's context.[202] One commenter saw proposed Item 106(b) as counteracting the streamlining accomplished in the Commission's 2020 release modernizing Regulation S-K.[203]

Some commenters offered suggestions to narrow proposed Item 106(b) to address their concerns. On proposed paragraph (b)(1), one commenter recommended allowing a registrant to forgo describing its risk assessment program if it confirms that it "uses best practices and standards" to identify and protect against cybersecurity risks and detect and respond to such events.[204] On proposed paragraph (b)(3), a few commenters said that registrants should be required to disclose only high-level information relating to third parties, such as confirmation that policies and procedures are appropriately applied to third-party selection and oversight, and should not have to identify the third parties or discuss the underlying mechanisms, controls, and contractual requirements.[205]

Some commenters opposed proposed paragraph (b)(6)'s requirement to discuss whether "previous cybersecurity incidents informed changes in the registrant's governance, policies and procedures, or technologies" entirely, stating it would undermine a registrant's cybersecurity.[206] One commenter recommended the proposed (b)(6) disclosure be required only at a high level, without specific details,[207] while two commenters appeared to propose only requiring disclosure

---

202 *See* letters from BPI et al.; Chamber; EIC; Nareit; NRF; NYSE; SCG; SIFMA; Virtu.

203 *See* letter from Nasdaq (citing *Modernization of Regulation S-K Items 101, 103, and 105*, Release No. 33-10825 (Aug. 26, 2020) [85 FR 63726 (Oct. 8, 2020)]).

204 *See* letter from Cybersecurity Coalition.

205 *See* letters from BPI et al.; Chamber; SIFMA. Other commenters supported the level of detail required in (b)(3). *See* letters from AICPA; PRI.

206 *See* letters from ITI; SCG; Tenable.

207 *See* letter from Cybersecurity Coalition.

as it pertains to previous material incidents.[208] Commenters suggested a materiality filter for proposed paragraph (b)(7)'s requirement to discuss whether "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," so that the requirement would apply only where a registrant has been materially affected or is reasonably likely to be materially affected.[209]

More broadly, one commenter recommended replacing the rule's references to "policies and procedures" with "strategy and programs," because in the commenter's experience companies may not codify their cybersecurity strategy in the same way they codify other compliance policies and procedures.[210] One commenter also suggested offering companies the choice to place the proposed Item 106(b) disclosures in either the Form 10-K or the proxy statement.[211]

Several commenters supported requiring registrants that lack cybersecurity policies and procedures to explicitly say so, commenting, for example, that "investors should not be left to intuit the meaning of a company's silence in its disclosures."[212] One commenter further stated that registrants should be required to explain why they have not adopted cybersecurity policies and procedures.[213] By contrast, two commenters opposed requiring registrants that lack

---

208 *See* letters from AGA/INGA; American Public Gas Association ("APGA").

209 *See* letter from PWC.

210 *See* letter from Prof. Perullo.

211 *See* letter from Nasdaq.

212 *See* letters from Blue Lava; CSA; Cybersecurity Coalition; ITI; NASAA; Prof. Perullo; Tenable. The quoted language is from NASAA's letter. *See also* IAC Recommendation (recommending "that issuers that have not developed any cybersecurity policies or procedures be required to make a statement to that effect" because "the vast majority of investors . . . would view the complete absence of cybersecurity risk governance as overwhelmingly material to investment decision-making").

213 *See* letter from NASAA.

cybersecurity policies and procedures to explicitly say so,[214] with one commenter saying that "a threat actor may target registrants they perceive to have unsophisticated cybersecurity programs,"[215] and the other commenter saying "it is highly unlikely that any SEC registrants would not have 'established any cybersecurity policies and procedures."[216]

In response to the Commission's request for comment about whether to require a registrant to specify whether any cybersecurity assessor, consultant, auditor, or other service provider that it relies on is through an internal function or through an external third-party service provider, several commenters opposed the idea as not useful, with one saying that "a significant majority—possibly the entirety—of SEC registrants" rely on third-party service providers for some portion of their cybersecurity.[217] Conversely, another commenter supported the third-party specification, and suggested requiring registrants to name the third parties, as over time, this would create more transparency in whether breaches correlate with specific third parties.[218]

Commenters also offered a range of recommended additions to the rule. One commenter recommended modifying proposed paragraph (b)(1) to require registrants to specify whether their cybersecurity programs assess risks continuously or periodically, arguing the latter approach leaves companies more exposed.[219] The same commenter suggested paragraph (b)(2) require "a description of the class of services and solutions" provided by third parties.[220]

---

214 *See* letters from EIC; IIA.

215 *See* letter from EIC.

216 *See* letter from IIA.

217 *See* letters from BCS; Chevron; EIC; IIA; Prof. Perullo. The quoted language is from the letter of IIA.

218 *See* letter from Blue Lava.

219 *See* letter from Tenable.

220 *Id.*

A few commenters recommended that we direct registrants to quantify their cybersecurity risk exposure through independent risk assessments.[221] Similarly, one commenter urged us to require registrants to explain how they quantify their cybersecurity risk,[222] while another said we should set out quantifiable metrics against which companies measure their cybersecurity systems, though it did not specify what these metrics should be.[223] Two commenters suggested that we require companies to disclose whether their cybersecurity programs have been audited by a third party.[224] And one commenter recommended that we require registrants to disclose whether they use the cybersecurity framework of the National Institute of Standards and Technology ("NIST"), to ease comparison of registrant risk profiles.[225]

c. Final Amendments

We continue to believe that investors need information on registrants' cybersecurity risk management and strategy, and that uniform, comparable, easy to locate disclosure will not emerge absent new rules. Commenters raised concerns with proposed Item 106(b)'s security implications and what they saw as its prescriptiveness. We agree that extensive public disclosure on how a company plans for, defends against, and responds to cyberattacks has the potential to advantage threat actors. Similarly, we acknowledge commenters' concerns that the final rule could unintentionally affect a registrant's risk management and strategy decision-making. In response to those comments, we confirm that the purpose of the rules is, and was at proposal, to inform investors, not to influence whether and how companies manage their cybersecurity risk.

---

221 *See* letters from BitSight; Kovrr Risk Modeling Ltd.; SecurityScorecard.

222 *See* letter from Safe Security.

223 *See* letter from FDD.

224 *See* letters from BCS; Better Markets.

225 *See* letter from SandboxAQ. This commenter also recommended registrants be required to disclose whether they use post-quantum cryptography as part of their risk mitigation efforts.

Additionally, to respond to commenters' concerns about security, the final rules eliminate or narrow certain elements from proposed Item 106(b). We believe the resulting rule requires disclosure of information material to the investment decisions of investors, in a way that is comparable and easy to locate, while steering clear of security sensitive details.

As adopted, 17 CFR 229.106(b)(1) (Regulation S-K "Item 106(b)(1)") requires a description of "the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes." We believe this revised formulation of the rule should help avoid levels of detail that may go beyond information that is material to investors and address commenters' concerns that those details could increase a company's vulnerability to cyberattack. We have also substituted the term "processes" for the proposed "policies and procedures" to avoid requiring disclosure of the kinds of operational details that could be weaponized by threat actors, and because the term "processes" more fully compasses registrants' cybersecurity practices than "policies and procedures," which suggest formal codification.[226] We still expect the disclosure to allow investors to ascertain a registrant's cybersecurity practices, such as whether they have a risk assessment program in place, with sufficient detail for investors to understand the registrant's cybersecurity risk profile. The shift to "processes" also obviates the question of whether to require companies that do not have written policies and procedures to disclose that fact. We believe that, to the extent a company discloses that it faces a material

[226] *See* letter from Prof. Perullo (distinguishing the formality of "policies and procedures" from the informality of "strategy or program"). We have adopted "processes" in place of the commenter's suggestion of "strategy or program" because "processes" is broader and commonly understood. We decline the suggestion from another commenter to allow registrants to avoid this disclosure altogether by confirming they adhere to "best practices and standards," because there is no single set of widely accepted best practices and standards, and industry practices may evolve. *See* letter from Cybersecurity Coalition.

cybersecurity risk in connection with its overall disclosures of material risks,[227] an investor can ascertain whether such risks have resulted in the adoption of processes to assess, identify, and manage material cybersecurity risks based on whether the company also makes such disclosures under the final rules.

We have also added a materiality qualifier to the proposed requirement to disclose "risks from cybersecurity threats," and have removed the proposed list of risk types (i.e., "intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk"), to foreclose any perception that the rule prescribes cybersecurity policy. We continue to believe these are the types of risks that registrants may face in this context, and enumerate them here as guidance. We note that registrants will continue to tailor their cybersecurity processes to threats as they perceive them. The rule requires registrants to describe those processes insofar as they relate to material cybersecurity risks.

We have also revised Item 106(b)'s enumerated disclosure elements in response to commenters that raised concerns regarding the level of detail required by some elements of the proposal. Specifically, we are not adopting proposed paragraphs (4) (prevention and detection activities), (5) (continuity and recovery plans), and (6) (previous incidents). We have similarly revised proposed paragraph (3) to eliminate some of the detail it required, consistent with commenter suggestions to require only high-level disclosure regarding third-party service providers. The enumerated elements that a registrant should address in its Item 106(b) disclosure, as applicable, are:

[227] *See* Item 105 of Regulation S-K.

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

We have also revised the rule text to clarify that the above elements compose a non-exclusive list of disclosures; registrants should additionally disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes.

We have moved proposed paragraph (7) into a separate paragraph, at 17 CFR 229.106(b)(2) (Regulation S-K "Item 106(b)(2)"), instead of including it in the enumerated list in Item 106(b)(1), and have added a materiality qualifier in response to a comment.[228] Item 106(b)(2) requires a description of "[w]hether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how."[229]

The final rules will require disclosure of whether a registrant engages assessors, consultants, auditors, or other third parties in connection with their cybersecurity because we

---

[228] *See* letter from PWC.

[229] With respect to the Item 106(b)(2)'s requirement to describe any risks as a result of any previous cybersecurity incidents, *see supra* Section II.B.3 for a discussion of the duties to correct or update prior disclosure that registrants may have in certain circumstances. As we note in that section, registrants should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

believe it is important for investors to know a registrant's level of in-house versus outsourced cybersecurity capacity. We understand that many registrants rely on third-party service providers for some portion of their cybersecurity, and we believe this information is accordingly necessary for investors to assess a company's cybersecurity risk profile in making investment decisions. However, we are not persuaded, as one commenter contended, that registrants should be required to name the third parties (though they may choose to do so), because we believe this may magnify concerns about increasing a company's cybersecurity vulnerabilities. For the same reason, we decline the commenter suggestion to require a description of the services provided by third parties.

We are also not persuaded that risk quantification or other quantifiable metrics are appropriate as mandatory elements of a cybersecurity disclosure framework. While such metrics may be used by registrants and investors in the future, commenters did not identify any such metrics that would be appropriate to mandate at this time. Additionally, to the extent that a registrant uses any quantitative metrics in assessing or managing cybersecurity risks, it may disclose such information voluntarily. For similar reasons, we decline commenters' recommendations to require disclosure of independent assessments and audits, as well as commenters' recommendations on disclosure of use of the NIST framework, and on distinguishing between continuous and periodic risk assessment.

We decline the commenter suggestion to allow Item 106(b) disclosure to be provided in the proxy statement, as the proxy statement is generally confined to information pertaining to the election of directors. We are also not requiring Item 106 disclosures in registration statements as recommended by the IAC, consistent with our efforts to reduce the burdens associated with the

final rule. However, as discussed further below,[230] we reiterate the Commission's guidance from the 2018 Interpretive Release that "[c]ompanies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements."[231] Finally, we note that registrants may satisfy the Item 106 disclosure requirements through incorporation by reference pursuant to 17 CFR 240.12b-23 ("Rule 12b-23").[232]

2. Governance

a. Proposed Amendments

The Commission proposed to add 17 CFR 229.106(c) (Regulation S-K "Item 106(c)") to require a description of management and the board's oversight of a registrant's cybersecurity risk. This information would complement the proposed risk management and strategy disclosure by clarifying for investors how a registrant's leadership oversees and implements its cybersecurity processes.[233] Proposed 17 CFR 229.106(c)(1) (Regulation S-K "Item 106(c)(1)") would focus on the board's role, requiring discussion, as applicable, of:

- 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.

---

230 *See infra* text accompanying notes 355 and 356.

231 2018 Interpretive Release at 8168.

232 As required by Rule 12b-23, in order to incorporate information by reference in answer, or partial answer, to Item 106, a registrant must, among other things, include an active hyperlink if the information is publicly available on EDGAR.

233 Proposing Release at 16600.

Proposed 17 CFR 229.106(c)(2) (Regulation S-K "Item 106(c)(2)") meanwhile would require a description of 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, including at a minimum discussion of:

- 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, 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;
- 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.

The Proposing Release explained that proposed Item 106(c)(1) would reinforce the Commission's 2018 Interpretive Release,[234] which said that disclosure on how a board engages management on cybersecurity helps investors assess the board's exercise of its oversight responsibility.[235] The Proposing Release noted that proposed Item 106(c)(2) would be of

[234] *Id.* (citing 2018 Interpretive Release at 8170).

[235] 2018 Interpretive Release at 8170.

importance to investors in that it would help investors understand how registrants are planning for cybersecurity risks and inform their decisions on how best to allocate their capital.[236]

b. Comments

A few commenters supported proposed Item 106(c) as providing investors with more uniform and informed understanding of registrants' governance of cybersecurity risks.[237] A number of commenters opposed proposed Item 106(c). They contended that the proposed Item 106(c) disclosures would be too granular to be decision-useful; instead, some of these commenters recommended that we limit the rule to a high-level explanation of management and the board's role in cybersecurity risk oversight.[238]

One commenter said proposed Item 106(c)(1) should be dropped because it duplicates existing 17 CFR 229.407(h) (Regulation S-K "Item 407(h)"), which requires reporting of material information regarding a board's leadership structure and role in risk oversight, including how it administers its oversight function.[239] Others saw similarities with Item 407(h) as well and suggested instead that proposed Item 106(c) be subsumed into Item 407, thus co-locating governance disclosures.[240]

In response to a request for comment in the Proposing Release on whether the Commission should expressly provide for the use of hyperlinks or cross-references in Item 106, one commenter supported the use of hyperlinks and cross-references, but sought clarification of

---

236 Proposing Release at 16600.

237 *See*, *e.g.*, letters from Better Markets; CalPERS.

238 *See* letters from ABA; AGA/INGAA; EEI; Nareit; NYSE.

239 *See* letter from Davis Polk. The commenter went on to say that, to the extent Item 106(c) requires disclosure of immaterial information regarding the board, it should be dropped.

240 *See* letters from ABA; BDO; PWC.

whether the practice is already permitted under Commission rules.[241] Another commenter opposed, saying Item 407(h)'s more general discussion of board governance is distinct from Item 106(c)(1)'s specific focus on cybersecurity.[242] The commenter cautioned that allowing registrants to employ hyperlinks and cross-references in Item 106 would lead to "less detail," resulting in disclosure insufficient to investor needs.[243]

One commenter recommended that we move proposed Item 106(c)(2) to the enumerated list of topics called for in proposed Item 106(b).[244] Another commenter suggested expanding the rule to include disclosure of management and staff training on cybersecurity, asserting that the information is useful to investors because policies depend on staff for successful implementation.[245] Two commenters suggested allowing the Item 106(c) disclosures to be made in the proxy statement.[246]

c. Final Amendments

In response to comments, and aligned with our changes to Item 106(b), we have streamlined Item 106(c) to require disclosure that is less granular than proposed. Under Item 106(c)(1) as adopted, registrants must "[d]escribe the board's oversight of risks from cybersecurity threats," and, if applicable, "identify any board committee or subcommittee responsible" for such oversight "and describe the processes by which the board or such committee is informed about such risks." We have removed proposed Item 106(c)(1)(iii), which had covered whether and how the board integrates cybersecurity into its business strategy, risk

241 *See* letter from E&Y.

242 *See* letter from Tenable.

243 *Id.*

244 *See* letter from Davis Polk.

245 *See* letter from PRI.

246 *See* letters from Business Roundtable; Nasdaq.

management, and financial oversight. While we have also removed the proposed Item 106(c)(1)(ii) requirement to disclose "the frequency of [the board or committee's] discussions" on cybersecurity, we note that, depending on context, some registrants' descriptions of the processes by which their board or relevant committee is informed about cybersecurity risks may include discussion of frequency.[247]

Given these changes, we find that Item 407(h) and Item 106(c)(1) as adopted serve distinct purposes and should not be combined, as suggested by some commenters—the former requires description of the board's leadership structure and administration of risk oversight generally, while the latter requires detail of the board's oversight of specific cybersecurity risk. As noted by one commenter,[248] to the extent these disclosures are duplicative, a registrant would be able to incorporate such information by reference.[249]

We have also modified Item 106(c)(2) to add a materiality qualifier, to make clear that registrants must "[d]escribe management's role in assessing and managing the registrant's *material* risks from cybersecurity threats" (emphasis added).[250] The enumerated disclosure elements now constitute a "non-exclusive list" registrants should consider including. We have revised the first element to require the disclosure of management positions or committees "responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise." Because this

---

247 For example, if the board or committee relies on periodic (e.g., quarterly) presentations by the registrant's chief information security officer to inform its consideration of risks from cybersecurity threats, the registrant may, in the course of describing those presentations, also note their frequency.

248 *See* letter from E&Y.

249 Rule 12b-23.

250 We have not added a materiality qualifier to Item 106(c)(1) because, if a board of directors determines to oversee a particular risk, the fact of such oversight being exercised by the board is material to investors. By contrast, management oversees many more matters and management's oversight of non-material matters is likely not material to investors, so a materiality qualifier is appropriate for Item 106(c)(2).

requirement would typically encompass identification of whether a registrant has a chief information security officer, or someone in a comparable position, we are not adopting the proposed second element that would have specifically called for disclosure of whether the registrant has a designated chief information security officer. Given our purpose of streamlining the disclosure requirements, we also are not adopting the proposed requirement to disclose the frequency of management-board discussions on cybersecurity, though, as noted above, discussion of frequency may in some cases be included as part of describing the processes by which the board or relevant committee is informed about cybersecurity risks in compliance with Item 106(c)(1), to the extent it is relevant to an understanding of the board's oversight of risks from cybersecurity threats.

Thus, as adopted, Item 106(c)(2) directs registrants to consider disclosing the following as part of a description of management's role in assessing and managing the registrant's material risks from cybersecurity threats:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
- The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

As many commenters recommended, these elements are limited to disclosure that we believe balances investors' needs to understand a registrant's governance of risks from cybersecurity threats in sufficient detail to inform an investment or voting decision with concerns

that the proposal could inadvertently pressure registrants to adopt specific or inflexible cybersecurity-risk governance practices or organizational structures. We do not believe these disclosures should be subsumed into Item 106(b), as one commenter recommended, because identifying the management committees and positions responsible for risks from cybersecurity threats is distinct from describing the cybersecurity practices management has deployed. We also decline the commenter suggestion to require disclosure of management and staff training on cybersecurity; registrants may choose to make such disclosure voluntarily. Finally, we decline the commenter suggestion to allow Item 106(c) disclosure to be provided in the proxy statement; governance information in the proxy statement is generally meant to inform shareholders' voting decisions, whereas Item 106(c) disclosure informs investors' assessment of investment risk.

3. Definitions

a. Proposed Definitions

The Commission proposed to define three terms to delineate the scope of the amendments: "cybersecurity incident," "cybersecurity threat," and "information systems."[251] Proposed 229 CFR 229.106(a) (Regulation S-K "Item 106(a)") would define them as follows:

- *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.

[251] Proposing Release at 16600-16601.

- *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.

As noted above, the Commission explained that what constitutes a "cybersecurity incident" should be construed broadly, encompassing a range of event types.[252]

b. Comments

Most commenters that offered feedback on the proposed definitions suggested narrowing them in some fashion. On "cybersecurity incident," many commenters urged limiting the definition to cases of actual harm, thereby excluding incidents that had only the potential to cause harm.[253] They suggested accomplishing this by replacing "jeopardizes" with phrases such as "adversely affects" or "results in substantial loss of."[254] One of these commenters noted that such a change would more closely align the definition with that in CIRCIA.[255] Other commenters objected to the definition's use of "any information" as overbroad, saying it would lead to inconsistent application.[256] One commenter sought clarification of whether the definition encompasses accidental incidents, such as chance technology outages, that do not involve a

252 *Id.* at 16601.

253 *See* letters from ABA; BPI et al.; Chamber et al.; Davis Polk; Enbridge; FDD; FEI; Hunton; PWC; SCG; SIFMA.

254 *See* letters from BPI et al.; Hunton.

255 *See* letter from BPI et al. ("The word 'jeopardizes' should be replaced with 'results in substantial loss of' to capture incidents that are causing some actual harm, and to better harmonize the definition with the reporting standard set forth by Congress in CIRCIA.").

256 *See* letters from Deloitte; SIFMA.

malicious actor,[257] while another commenter advocated broadening the definition to any incident materially disrupting operations, regardless of what precipitated it.[258]

On "cybersecurity threat," commenters urged narrowing the rule by replacing the language "may result in" with "could reasonably be expected to result in" or some other probability threshold.[259] One stated that "the use of a 'may' standard establishes an unhelpfully low standard that would require registrants to establish policies and procedures to identify threats that are potentially overbroad and not appropriately tailored to those threats that are reasonably foreseeable."[260] In a similar vein, two commenters objected to the language "any potential occurrence" as over-inclusive and lacking "instructive boundaries."[261]

On "information systems," many commenters favored replacing "owned or used by" with "owned or operated by," "owned or controlled by," or like terms, so that registrants' reporting obligations stop short of incidents on third-party information systems.[262] A few commenters said the definition could be construed to cover hard-copy information and should be revised to foreclose such a reading.[263]

More broadly, many commenters advised the Commission to align these definitions with comparable definitions in other Federal laws and regulations, such as CIRCIA and NIST.[264] One

---

257 *See* letter from CSA.

258 *See* letter from Crindata.

259 *See* letters from Chevron; Debevoise; NYC Bar.

260 *See* letter from Debevoise.

261 *See* letters from Chevron; Deloitte.

262 *See* letters from ABA; APCIA; Business Roundtable; Chamber; Cybersecurity Coalition; ISA; ITI; NAM; NDIA; Paylocity. Other commenters made similar arguments about third party systems without speaking specifically to the definition, saying, for example, that registrants may not have sufficient visibility into third-party systems and may be bound by confidentiality agreements. *See* letters from AIA; EIC; FAH; NMHC; SIFMA.

263 *See* letters from ABA; BPI et al.; Enbridge.

264 *See* letters from ABA; CAQ; Chevron; FEI; IC; IIA; Microsoft; PWC; SandboxAQ; SIFMA.

commenter explained that "[a]ligning definitions with those in existing federal laws and regulations would help ensure that the defined terms are consistently understood, interpreted and applied in the relevant disclosure."[265] However, another commenter cautioned against aligning with definitions, such as those of NIST, that were developed with a view toward internal risk management and response rather than external reporting; the commenter identified CIRCIA and the Federal banking regulators' definitions as more apposite.[266] One commenter noted that additional proposed defined terms were included in the Commission's rulemaking release *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*[267] that were not included in the Proposing Release and recommended that we "consider whether the defined terms should be consistent."[268]

In the Proposing Release, the Commission asked whether to define other terms used in the proposed amendments, and specifically sought comment on whether a definition of "cybersecurity" would be useful.[269] Several commenters supported defining "cybersecurity,"[270] reasoning, for example, that any rulemaking on cybersecurity should define that baseline term;[271] that, left undefined, the term would be open to varying interpretations;[272] and that details such as whether hardware is covered should be resolved.[273] Separately, two commenters recommended

---

265 *See* letter from ABA.

266 *See* letter from SCG.

267 Release No. 33-11028 (Feb. 9, 2022) [87 FR 13524 (Mar. 9, 2022)].

268 *See* letter from Deloitte.

269 Proposing Release at 16601.

270 *See* letters from BCS; Blue Lava; EIC; R. Hackman; R Street.

271 *See* letter from R Street.

272 *See* letter from Blue Lava.

273 *See* letter from BCS.

the Commission define "operational technology,"[274] with one explaining that the "proposed definitions understandably focus on data breaches, which are a major cybersecurity threat, but we believe an operational technology breach could have even more detrimental effects in certain cases (such as for ransomware attacks that have impacted critical infrastructure) and warrants disclosure guidance from the Commission."[275]

Several commenters also sought either a formal definition or more guidance on the term "material" specific to the cybersecurity space.[276] Some read the proposal, particularly the incident examples provided in the Proposing Release, as lowering the bar for materiality and being overly subjective, which they indicated may result in over-reporting of cybersecurity incidents or introduce uncertainty, and they urged the Commission to affirm the standard materiality definition.[277] Another commenter sought cybersecurity-specific guidance on materiality, including "concrete thresholds to assist registrants in determining materiality."[278] A few commenters recommended conditioning the materiality determination on the underlying information being verified to "a high degree of confidence" and "unlikely to materially change,"[279] while one commenter looked to replace materiality altogether with a significance standard like that in CIRCIA.[280]

c. Final Definitions

---

274 *See* letters from Chevron; EIC.

275 *See* letter from Chevron.

276 *See* letters from ACLI; AIC; AICPA; APCIA; Bitsight; Harry Broadman, Eric Matrejek, and Brad Wilson ("Broadman et al."); Debevoise; EIC; International Information System Security Certification Consortium ("ISC2"); M. Barragan; NYC Bar; Prof. Perullo; R Street; SIFMA; TransUnion; Virtu.

277 *See* letters from APCIA; ACLI; EIC; Virtu.

278 *See* letter from SIFMA.

279 *See* letters from Debevoise; NYC Bar. *See also* letter from AIC (suggesting "unlikely to change," without "materially").

280 *See* letter from National Electrical Manufacturers Association ("NEMA").

We are adopting definitions for "cybersecurity incident," "cybersecurity threat," and "information systems" largely as proposed, with three modifications.

First, on "cybersecurity incident," we are adding the phrase "or a series of related unauthorized occurrences" to the "cybersecurity incident" definition. This reflects our guidance in Section II.B.3 above that a series of related occurrences may collectively have a material impact or reasonably likely material impact and therefore trigger Form 8-K Item 1.05, even if each individual occurrence on its own would not rise to the level of materiality. Second, we are making a clarifying edit to "information systems." Some commenters said the definition could be construed to cover hard-copy resources.[281] We recognize that reading is possible, if unlikely and unintended, and we are therefore inserting "electronic" before "information resources," to ensure the rules pertain only to electronic resources. Third, we are making minor revisions to the "cybersecurity threat" definition for clarity and to better align it with the "cybersecurity incident" definition.

Accordingly, the definitions are as follows:

- *Cybersecurity incident* means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.
- *Cybersecurity threat* means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

[281] *See* letters from ABA; BPI et al.; Enbridge.

- *Information systems* means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

We recognize commenters' concern regarding the term "jeopardizes" in the proposed "cybersecurity incident" definition and the resulting scope of the definition. Nonetheless, we note that the definition is not self-executing; rather it is operationalized by Item 1.05, which is conditioned on the incident having been material to the registrant. Typically that would entail actual harm, though the harm may sometimes be delayed, and a material cybersecurity incident may not result in actual harm in all instances. For example, a company whose intellectual property is stolen may not suffer harm immediately, but it may foresee that harm will likely occur over time as that information is sold to other parties, such that it can determine materiality before the harm occurs. The reputational harm from a breach may similarly increase over time in a foreseeable manner. There may also be cases, even if uncommon, where the jeopardy caused by a cybersecurity incident materially affects the company, even if the incident has not yet caused actual harm. In such circumstances, we believe investors should be apprised of the material effects of the incident. We are therefore retaining the word "jeopardizes" in the definition.

We are not persuaded that the proposed "cybersecurity incident" definition's use of "any information" would lead to inconsistent application of the definition among issuers or cause a risk of over-reporting, as suggested by some commenters. As noted above, the "cybersecurity incident" definition is operationalized by Item 1.05. Item 1.05 does not require disclosure

whenever "any information" is affected by an intruder. Disclosure is triggered only when the resulting effect of an incident on the registrant is material.

We are also retaining "unauthorized" in the incident definition as proposed. In general, we believe that an accidental occurrence is an unauthorized occurrence. Therefore, we note that an accidental occurrence may be a cybersecurity incident under our definition, even if there is no confirmed malicious activity. For example, if a company's customer data are accidentally exposed, allowing unauthorized access to such data, the data breach would constitute a "cybersecurity incident" that would necessitate a materiality analysis to determine whether disclosure under Item 1.05 of Form 8-K is required.

On "cybersecurity threat," we appreciate commenters' concerns with the proposed definition's use of "may result in" and "any potential occurrence." Unlike with "cybersecurity incident," where the interplay of the proposed definition with proposed Item 1.05 ensured only material incidents would become reportable, proposed Item 106(b)'s reference to "the identification and management of risks from cybersecurity threats" was not qualified by materiality. We are therefore adding a materiality condition to Item 106(b). As adopted, Item 106(b) will require disclosure of registrants' processes to address the material risks of potential occurrences that could reasonably result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of a registrant's information systems. Given the addition of a materiality condition to Item 106(b), we do not believe that further revision to the "cybersecurity threat" definition is warranted.

On "information systems," we decline to change "owned or used by" to "owned or operated by," "owned or controlled by," or similar terms advanced by commenters. Commenters recognized that "used by" covers information resources owned by third parties. That is by

design: covering third party systems is essential to the working of Item 106 of Regulation S-K and Item 1.05 of Form 8-K. As we explain above, in Section II.A.3, the materiality of a cybersecurity incident is contingent neither on where the relevant electronic systems reside nor on who owns them, but rather on the impact to the registrant. We do not believe that a reasonable investor would view a significant data breach as immaterial merely because the data are housed on a cloud service. If we were to remove "used by," a registrant could evade the disclosure requirements of the final rules by contracting out all of its information technology needs to third parties. Accordingly, the definition of "information systems" contemplates those resources owned by third parties and used by the registrant, as proposed.

In considering commenters' suggestion to align our definitions with CIRCIA, NIST, and other Federal regulations, we observe that there is no one standard definition for these terms, and that regulators have adopted definitions based on the specific contexts applicable to their regulations. Nonetheless, we also observe that the final "cybersecurity incident" definition is already similar to the CIRCIA and NIST incident definitions, in that all three focus on the confidentiality, integrity, and availability of information systems.[282] Our definition of "information systems" also tracks CIRCIA and NIST, as all three cover "information resources" that are "organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition" of information.[283] Of course, the definitions do not match precisely, but some variation is inevitable where various Federal laws and regulations have different purposes, contexts, and goals. We therefore find that further alignment is not needed.

---

[282] For CIRCIA, *see supra* note 19, at sec. 103, 136 Stat. 1039; and 6 U.S.C. 681b(c)(2)(A)(i). For NIST, *see Incident*, Glossary, NIST COMPUTER SECURITY RESOURCE CENTER, *available at https://csrc.nist.gov/glossary/term/incident*.

[283] For CIRCIA, *see supra* note 19, at sec. 103, 136 Stat. 1039; and 44 U.S.C. 3502(8). For NIST, *see Information System*, Glossary, NIST COMPUTER SECURITY RESOURCE CENTER, *available at https://csrc.nist.gov/glossary/term/information_system*.

We decline to define any other terms. We acknowledge commenters who asked for additional guidance regarding the application of a materiality determination to cybersecurity or sought to replace materiality with a significance standard. As noted in the Proposing Release, however, we expect that registrants will apply materiality considerations as would be applied regarding any other risk or event that a registrant faces. Carving out a cybersecurity-specific materiality definition would mark a significant departure from current practice, and would not be consistent with the intent of the final rules.[284] Accordingly, we reiterate, consistent with the standard set out in the cases addressing materiality in the securities laws, that information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important"[285] in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."[286] Because materiality's focus on the total mix of information is from the perspective of a reasonable investor, companies assessing the materiality of cybersecurity incidents, risks, and related issues should do so through the lens of the reasonable investor. Their evaluation should take into consideration all relevant facts and circumstances, which may involve consideration of both quantitative and qualitative factors. Thus, for example, when a registrant experiences a data breach, it should consider both the immediate fallout and any longer term effects on its operations, finances, brand perception, customer relationships, and so on, as part of its materiality analysis. We also note that, given the fact-specific nature of the materiality determination, the same incident that affects multiple

---

[284] *See, e.g.*, *Basic Inc. v. Levinson*, 485 U.S. 224, 236 (1988) ("[a]ny approach that designates a single fact or occurrence as always determinative of an inherently fact-specific finding such as materiality, must necessarily be overinclusive or underinclusive").

[285] *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976); *Matrixx Initiatives v. Siracusano*, 563 U.S. 27, 38-40 (2011); *Basic*, 485 U.S. at 240.

[286] *Id.* See also the definition of "material" in 17 CFR 230.405 [Securities Act Rule 405]; 17 CFR 240.12b-2 [Exchange Act Rule 12b-2].

registrants may not become reportable at the same time, and it may be reportable for some registrants but not others.

We also decline to separately define "cybersecurity," as suggested by some commenters. We do not believe such further definition is necessary, given the broad understanding of this term. To that end, we note that the cybersecurity industry itself appears not to have settled on an exact definition, and because the field is quickly evolving and is expected to continue to evolve over time, any definition codified in regulation could soon become stale as technology develops. Likewise, the final rules provide flexibility by not defining "cybersecurity," allowing a registrant to determine meaning based on how it considers and views such matters in practice, and on how the field itself evolves over time.

We decline to define "operational technology" as suggested by some commenters because the term does not appear in the rules we are adopting.

D. Disclosure Regarding the Board of Directors' Cybersecurity Expertise

1. Proposed Amendments

Congruent with proposed Item 106(c)(2) on the board's oversight of cybersecurity risk, the Commission proposed adding 17 CFR 229.407(j) (Regulation S-K "Item 407(j)") to require disclosure about the cybersecurity expertise, if any, of a registrant's board members.[287] The proposed rule did not define what constitutes expertise, given the wide-ranging nature of cybersecurity skills, but included a non-exclusive list of criteria to consider, such as prior work experience, certifications, and the like. As proposed, paragraph (j) would build on existing 17 CFR 229.401(e) (Regulation S-K "Item 401(e)") (business experience of directors) and Item 407(h) (board risk oversight), and would be required in the annual report on Form 10-K and in

[287] Proposing Release at 16601.

the proxy or information statement when action is to be taken on the election of directors. Thus, the Proposing Release said, proposed Item 407(j) would help investors in making both investment and voting decisions.[288]

The Commission also proposed to include a safe harbor in 17 CFR 229.407(j)(2) (Regulation S-K "Item 407(j)(2)") providing that any directors identified as cybersecurity experts would not be deemed experts for liability purposes, including under Section 11 of the Securities Act.[289] This was intended to clarify that identified directors do not assume any duties, obligations, or liabilities greater than those assumed by non-expert directors.[290] Nor would such identification decrease the duties, obligations, and liabilities of non-expert directors relative to identified directors.[291]

2. Comments

Proposed Item 407(j) garnered significant comment. Supporters wrote that understanding a board's level of cybersecurity expertise is important to assessing a company's ability to manage cybersecurity risk.[292] For example, one commenter said "[b]oard cybersecurity expertise serves as a useful starting point for investors to assess a company's approach to cybersecurity;"[293] while another commenter said investors need the Item 407(j) disclosure "[t]o cast informed votes on directors."[294] One comment letter submitted an academic study by the

---

288 *Id.*

289 *Id.* at 16602.

290 *Id.*

291 *Id.*

292 *See* letters from O. Borges; CalPERS; Prof. Choudhary; CII; Digital Directors Network ("DDN"); ISC2; Prof. Lowry et al.; NACD; PRI; SANS Institute; SM4RT Secure.

293 *See* letter from PRI.

294 *See* letter from CII.

authors of the letter and noted that its findings "underscore the importance of understanding the role of boards in cybersecurity oversight."[295]

By contrast, many commenters argued cybersecurity risk is not intrinsically different from other risks that directors assess with or without specific technical expertise.[296] For example, one reasoned that, given the "ever-changing range of risks confronting a company," directors require "broad-based skills in risk and management oversight, rather than subject matter expertise in one particular type of risk."[297] Commenters also predicted the disclosure requirement would pressure companies to retain cybersecurity experts on their board, and submitted there is not enough cybersecurity talent in the marketplace at this time for all or most companies to do so.[298] One of these commenters further contended that finding such expertise will be harder for smaller reporting companies.[299] Another commenter warned that, given the current cybersecurity talent pool, the end result may be lower diversity on boards;[300] and one said hiring cybersecurity experts to the board may come at the expense of spending on a company's cybersecurity defenses.[301] Commenters also expressed concern that the identified expert

---

295 *See* letter from Prof. Lowry et al.

296 *See* letters from ABA; ACC; AGA/INGAA; AICPA; Auto Innovators; BDO; BPI et al.; Business Roundtable; CAQ; CBA; Chamber; CTA; CTIA; Davis Polk; Deloitte; EEI; EIC; Hunton; ITI; IC; LTSE; Microsoft; Nareit; NAM; NDIA; NRA; NYSE; PPG; Safe Security; SCG; SIFMA; TechNet; USTelecom; Virtu; Wilson Sonsini. *See also* IAC Recommendation.

297 *See* letter from ABA.

298 *See* letters from ACC; APCIA; BIO; Blue Lava; Chamber; FDD; ITI (May 9, 2022); NDIA; NYSE; SCG (May 9, 2022). In this vein, a commenter requested the Commission affirm Item 407(j) is only a disclosure provision and is not intended to mandate cybersecurity expertise on the board. *See* letter from Federated Hermes.

299 *See* letter from BIO.

300 *See* letter from Chamber ("An unintended consequence of the SEC proposal is likely to create new barriers for underrepresented groups to move into cybersecurity leadership roles largely due to the expense of obtaining credentials and other formal certifications. The costs associated with obtaining cybersecurity-related degrees and other credentials could hinder the advancement of individuals who could otherwise rise through the ranks within the field of cybersecurity.").

301 *See* letter from Wilson Sonsini.

directors would face elevated risks, such as being targeted by nation states for surveillance or hackers attempting to embarrass them, thus creating a disincentive to board service.[302]

More generally, sentiment among those opposed to Item 407(j) was that the rule is overly prescriptive and in effect would direct how companies operate their cybersecurity programs.[303] As an alternative, some commenters pushed for other ways to show competency, such as identifying outside experts the board relies on for cybersecurity expertise, disclosing how frequently the board meets with the chief information security officer, listing relevant director training, and relying on adjacent technology skills.[304]

Whether they supported or opposed the proposed disclosure requirement, commenters largely endorsed the proposed Item 407(j)(2) safe harbor; its absence, they said, could make candidates with cybersecurity expertise reluctant to serve on boards.[305] Two commenters requested the Commission define "cybersecurity expertise;"[306] one of them said being "duly accredited and certified as a cybersecurity professional" should be a prerequisite, and posited specific industry certifications to establish expertise.[307] Another commenter suggested adding participation in continuing education to the 17 CFR 229.407(j)(1)(i) factors considered in assessing expertise.[308]

---

302 *See* letters from BIO; Chevron; EEI; EIC; Hunton; Profs. Rajgopal & Sharp.

303 *See*, *e.g.*, letter from ACC.

304 *See* letters from AGA/INGAA; BPI et al.; Business Roundtable; DDN; LTSE; PRI; Wilson Sonsini.

305 *See* letters from ABA; BIO; CII; CSA; A. Heighington; NACD; Paylocity; Prof. Perullo.

306 *See* letters from Federated Hermes; ISC2.

307 *See* letter from ISC2.

308 *See* letter from SandboxAQ.

3. Final Amendments

After considering the comments, we are not adopting proposed Item 407(j). We are persuaded that effective cybersecurity processes are designed and administered largely at the management level, and that directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise, as they do with other sophisticated technical matters. While we acknowledge that some commenters indicated that the proposed Item 407(j) information would be helpful to investors, we nonetheless agree that it may not be material information for all registrants. We believe investors can form sound investment decisions based on the information required by Items 106(b) and (c) without the need for specific information regarding board-level expertise. And to that end, a registrant that has determined that board-level expertise is a necessary component to the registrant's cyber-risk management would likely provide that disclosure pursuant to Items 106(b) and (c).

E. Disclosure by Foreign Private Issuers

1. Proposed Amendments

The Commission proposed to establish disclosure requirements for FPIs parallel to those proposed for domestic issuers in Regulation S-K Items 106 and 407(j) and Form 8-K Item 1.05.[309] Specifically, the Commission proposed to amend Form 20-F to incorporate the requirements of proposed Item 106 and 407(j) to disclose information regarding an FPI's cybersecurity risk management, strategy, and governance.[310] With respect to incident disclosure,

---

[309] Proposing Release at 16602. The Commission did not propose to amend Form 40-F, choosing rather to maintain the multijurisdictional disclosure system ("MJDS") whereby eligible Canadian FPIs use Canadian disclosure standards and documents to satisfy SEC registration and disclosure requirements.

[310] As noted in the Proposing Release, FPIs would include the expertise disclosure only in their annual reports, as they are not subject to Commission rules for proxies and information statements.

the Commission proposed to: (1) 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,[311] and (2) amend Form 20-F to require updated disclosure regarding incidents previously disclosed on Form 6-K.

2. Comments

A few commenters agreed that the Commission should not exempt FPIs from the proposed disclosure requirements, given they face the same threats as domestic issuers.[312] Another commenter said the Commission should not delay compliance for FPIs, for similar reasons.[313] On the other hand, one commenter said the proposal would disproportionately burden FPIs because, under its reading of the proposed amendment to General Instruction B, Form 6-K would require disclosure of all cybersecurity incidents, not just those that are material.[314] The commenter went on to say that the interplay of the European Union's Market Abuse Regulation ("MAR") would render the proposed Form 6-K amendment particularly taxing, because MAR requires immediate announcement of non-public price sensitive information.[315]

On MJDS filers, commenters endorsed the Commission's determination not to propose to amend Form 40-F, maintaining that Canadian issuers eligible to use MJDS should be permitted to follow their domestic disclosure standards, consistent with other disclosure requirements for those registrants.[316]

---

311 A registrant is required under Form 6-K to furnish copies of all information that it: (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.

312 *See* letters from CSA; Cybersecurity Coalition; Prof. Perullo; Tenable.

313 *See* letter from Crindata.

314 *See* letter from SIFMA.

315 *Id.*

316 *See* letters from ACLI; BCE; Cameco Corporation; CBA; Sun Life Financial Inc.

3. Final Amendments

We are adopting the Form 20-F and Form 6-K amendments as proposed, with modifications that are consistent with those being applied to Item 106 of Regulation S-K and Item 1.05 of Form 8-K. We continue to believe that FPIs' cybersecurity incidents and risks are not any less important to investors' capital allocation than those of domestic registrants. We also do not find that the Form 6-K amendments unduly burden FPIs. Importantly, the language the Commission proposed to add to General Instruction B ("cybersecurity incident") of Form 6-K would be modified by the existing language "that which is material with respect to the issuer and its subsidiaries concerning." Nonetheless, for added clarity, we are including the word "material" before "cybersecurity incident." Thus, for a cybersecurity incident to trigger a disclosure obligation on Form 6-K, the registrant must determine that the incident is material, in addition to meeting the other criteria for required submission of the Form.[317] Even registrants subject to the European Union's MAR will first have developed the relevant information for foreign disclosure or publication under MAR, so any added burden for preparing and furnishing the Form 6-K should be minor. As the Commission stated in the Proposing Release, we do not find reason to adopt prescriptive cybersecurity disclosure requirements for Form 40-F filers, given that the MJDS generally permits eligible Canadian FPIs to use Canadian disclosure standards and documents to satisfy the Commission's registration and disclosure requirements.[318] We note that such filers are already subject to the Canadian Securities Administrators' 2017 guidance on the disclosure of cybersecurity risks and incidents.[319]

---

317 *See supra* note 311 for the other criteria.

318 Proposing Release at 16603.

319 Canadian Securities Administrators, *CSA Multilateral Staff Notice 51-347 – Disclosure of cyber security risks and incidents* (Jan. 19, 2017).

F. Structured Data Requirements

1. Proposed Amendments

The Commission proposed to mandate that registrants tag the new disclosures in Inline XBRL, including by block text tagging narrative disclosures and detail tagging quantitative amounts.[320] The Proposing Release explained that the structured data requirements would make the disclosures more accessible to investors and other market participants and facilitate more efficient analysis.[321] The proposed requirements would not be unduly burdensome to registrants, the release posited, because they are similar to the Inline XBRL requirements for other disclosures.[322]

2. Comments

Commenters largely supported the proposal to require Inline XBRL tagging of the new disclosures, as structured data would enable automated extraction and analysis.[323] Opposition to the requirement centered on filer burden, including an argument that, given the time-sensitive nature of the Item 1.05 Form 8-K disclosure, mandating structured data tagging would unduly add to companies' burden in completing timely reporting.[324]

3. Final Amendments

After considering comments, we are adopting the structured data requirements as proposed, with a staggered compliance date of one year.[325] We are not persuaded that Inline

---

320 Proposing Release at 16603.

321 *Id.*

322 *Id.*

323 *See* letters from AICPA; CAQ; Crowe LLP; E&Y; FDD; K. Fuller; NACD; PWC; Professors Lawrence Trautman & Neal Newman; XBRL US.

324 *See* letters from NYC Bar; SFA.

325 We have incorporated modifications of a technical nature to the regulatory text.

XBRL tagging will unduly add to companies' burden in preparing and filing Item 1.05 Form 8-K in a timely fashion, and we believe such incremental costs are appropriate given the significant benefits to investors. Compared to the Inline XBRL tagging companies will already be performing for their financial statements, the tagging requirements here are less extensive and complex. Inline XBRL tagging will enable automated extraction and analysis of the information required by the final rules, allowing investors and other market participants to more efficiently identify responsive disclosure, as well as perform large-scale analysis and comparison of this information across registrants.[326] The Inline XBRL requirement will also enable automatic comparison of tagged disclosures against prior periods. If we were not to adopt the Inline XBRL requirement as suggested by some commenters, some of the benefit of the new rules would be diminished. However, we are delaying compliance with the structured data requirements for one year beyond initial compliance with the disclosure requirements. This approach should both help lessen any compliance burden and improve data.

G. Applicability to Certain Issuers

1. Asset-Backed Issuers

The Commission proposed to amend Form 10-K to clarify that an asset-backed issuer, as defined in 17 CFR 229.1101 (Regulation AB "Item 1101"), that does not have any executive officers or directors may omit the information required by proposed Item 106(c).[327] The Commission noted that asset-backed issuers would likewise be exempt from proposed Item

---

[326] These considerations are generally consistent with objectives of the recently enacted Financial Data Transparency Act of 2022, which directs the establishment by the Commission and other financial regulators of data standards for collections of information, including with respect to periodic and current reports required to be filed or furnished under Exchange Act Sections 13 and 15(d). Such data standards must meet specified criteria relating to openness and machine-readability and promote interoperability of financial regulatory data across members of the Financial Stability Oversight Council. *See* James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, P.L. 117-263, tit. LVIII, 136 Stat. 2395, 3421-39 (2022).

[327] Proposing Release at 16600.

407(j) pursuant to existing Instruction J to Form 10-K.[328] The Commission further requested comment on whether to generally exempt asset-backed issuers from the proposed rules.

One commenter stated that the proposed rules should not apply to issuers of asset-backed securities, given that they are limited purpose or passive special purpose vehicles with limited activities, no operations or businesses, and no information systems.[329] The commenter also opposed applying the proposed rules to other transaction parties (such as the sponsor, servicer, originator, and trustee), because such parties are neither issuers of nor obligors on an asset-backed security, and "it is extraordinarily unlikely that a transaction party's financial performance or position would be impacted by a cybersecurity incident to such an extent as to impede its ability to perform its duties and responsibilities to the securitization transaction."[330] The commenter acknowledged that cybersecurity disclosure rules may make sense for servicers of asset-backed securities, but counseled that any new rules should be tailored to such entities, rather than applying the proposed rules.[331]

We are exempting asset-backed securities issuers from the final rules.[332] We agree with the commenter that the final rules would not result in meaningful disclosure by asset-backed issuers. In particular, we are persuaded by the fact that asset-backed issuers are typically special purpose vehicles whose activities are limited to receiving or purchasing, and transferring or selling, assets to an issuing entity[333] and, accordingly, do not own or use information systems,

---

328 *Id.* at 16601.

329 *See* letter from SFA.

330 *Id.*

331 *Id.*

332 *See* General Instruction G to Form 8-K, and General Instruction J to Form 10-K.

333 *See* letter from SFA (citing the definitions contained in 17 CFR 229.1101(b), 17 CFR 230.191, and 17 CFR 240.3b-19).

whereas the final rules are premised on an issuer's ownership or use of information systems.[334] To the extent that a servicer or other party to an asset-backed security transaction is a public company, it will be required to comply with the final rules with respect to information systems it owns or uses. Therefore, an investor in an asset-backed security who wants to assess the cybersecurity of transaction parties will be able to do so for those that are public companies. The Commission may consider cybersecurity disclosure rules specific to asset-backed securities at a later date.

2. Smaller Reporting Companies

In the Proposing Release, the Commission did not include an exemption or alternative compliance dates or transition accommodations for smaller reporting companies, but it did request comment on whether to do so.[335] The Commission noted that smaller companies may face equal or greater cybersecurity risk than larger companies, such that cybersecurity disclosures may be particularly important for their investors.[336]

A few commenters advocated an exemption for smaller reporting companies, asserting that they face outsized costs from the proposal and lower cybersecurity risk.[337] And some commenters called for a longer compliance phase-in period for smaller reporting companies, to help them mitigate their cost burdens and benefit from the compliance and disclosure experience of larger companies.[338] Other commenters opposed an exemption for smaller reporting

---

334 The definition of "cybersecurity incident" focuses on "a registrant's information systems." Likewise, the definition of "cybersecurity threat" concerns "a registrant's information systems or any information residing therein."

335 Proposing Release at 16601.

336 *Id.* at 16613.

337 *See* letters from BIO; NDIA.

338 *See* letters from BIO; BDO; NACD; Nasdaq. In addition, the Commission's Small Business Capital Formation Advisory Committee highlights generally in its parting perspectives letter that "exemptions, scaling, and phase-

companies,[339] in part because they may face equal[340] or greater[341] cybersecurity risk than larger companies, or because investors' relative share in a smaller company may be higher, such that small companies' cybersecurity risk "may actually embody the most pressing cybersecurity risk to an investor."[342]

Consistent with the proposal, we decline to exempt smaller reporting companies. We believe the streamlined requirements of the final rules will help reduce some of the costs associated with the proposal for all registrants, including smaller reporting companies. Also, we do not believe that an additional compliance period is needed for smaller reporting companies with respect to Item 106, as this information is factual in nature regarding a registrant's existing cybersecurity strategy, risk management, and governance, and so should be readily available to those companies to assess for purposes of preparing disclosure. Finally, given the significant cybersecurity risks smaller reporting companies face and the outsized impacts that cybersecurity incidents may have on their businesses, their investors need access to timely disclosure on material cybersecurity incidents and the material aspects of their cybersecurity risk management and governance. However, we agree with commenters that stated smaller reporting companies would likely benefit from additional time to comply with the incident disclosure requirements.

---

ins for new requirements where appropriate, allows smaller companies to build their businesses and balance the needs of companies and investors while promoting strong and effective U.S. public markets." *See* Parting Perspectives Letter, U.S. Securities and Exchange Commission Small Business Capital Formation Advisory Committee (Feb. 28, 2023), *available at https://www.sec.gov/files/committee-perspectives-letter-022823.pdf*. *See also* U.S. Securities and Exchange Commission Office of the Advocate for Small Business Capital Formation, *Annual Report Fiscal Year 2022* ("2022 OASB Annual Report"), *available at https://www.sec.gov/files/2022-oasb-annual-report.pdf*, at 83 (recommending generally that in engaging in rulemaking that affects small businesses, the Commission tailor the disclosure and reporting framework to the complexity and size of operations of companies, either by scaling obligations or delaying compliance for the smallest of the public companies).

339 *See* letters from CSA; Cybersecurity Coalition; NASAA; Prof. Perullo; Tenable.

340 *See* letter from Cybersecurity Coalition.

341 *See* letters from NASAA and Tenable.

342 *See* letter from Prof. Perullo.

Accordingly, as discussed below, we are providing smaller reporting companies an additional 180 days from the non-smaller reporting company compliance date before they must begin complying with Item 1.05 of Form 8-K.

H. Need for New Rules and Commission Authority

Some commenters argued that the 2011 Staff Guidance and 2018 Interpretive Release are sufficient to compel adequate cybersecurity disclosure, obviating the need for new rules.[343] In this regard, two commenters highlighted the Proposing Release's statement that cybersecurity disclosures "have improved since the issuance of the 2011 Staff Guidance and the 2018 Interpretive Release."[344] Another commenter said that Commission staff's findings that certain cybersecurity incidents were reported in the media but not disclosed in a registrant's filings and that registrants' disclosures provide different levels of specificity suggested that "existing guidance is working, because each registrant should always be conducting an individualized, case-by-case analysis" and therefore disclosures "should expectedly vary significantly."[345] One commenter questioned whether the materials cited in the Proposing Release support the Commission's conclusion there that current cybersecurity reporting may be inconsistent, not timely, difficult to locate, and contain insufficient detail.[346] Two commenters recommended that the Commission "reemphasize" the prior guidance and "utilize its enforcement powers to ensure

---

343 *See* letters from BPI et al.; CTIA; ISA; ITI; SCG; SIFMA; Virtu.

344 *See* letters from Virtu (citing Proposing Release at 16594); BPI et al. (pointing to the Proposing Release's citation of 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/whatcompanies-are-disclosing-about-cybersecurity-riskand-oversight*).

345 *See* letter from ITI.

346 *See* letter from BPI et al. (discussing Moody's Investors Service, Research Announcement, *Cybersecurity disclosures vary greatly in high-risk industries* (Oct. 3, 2019)*;* NACD et al., *The State of Cyber-Risk Disclosures of Public Companies* (Mar. 2021), at 3).

public companies continue to report material cyber incidents."[347] One commenter provided the results from a survey it conducted of its members, finding that "only 10-20% of the 192 respondents reported that their shareholders have requested information or asked a question on" various cybersecurity topics, while "64.3% of the respondents indicated that their investors had not engaged with them" on those topics.[348] Another commenter pointed to a 2022 study finding that less than 1% of cybersecurity breaches are "material," and asserted that current disclosures adequately reflect such a level of material breaches.[349] Some commenters also stated that the Commission should forgo regulation of cybersecurity disclosure because other agencies' regulations are sufficient.[350]

Other commenters, by contrast, stated that the 2011 Staff Guidance and the 2018 Interpretive Release, while helpful, have not been sufficient to provide investors with the material information they need. One such commenter explained that "[t]he Commission's past guidance, while in line with our views, does not go far enough. The Proposed Rule is needed to provide clarity regarding what, when, and how to disclose material cybersecurity incident information . . . The improved standardization of disclosures included in the Proposed Rule adds clarity to the reporting process."[351] Another commenter stated that "[t]he lack of timely,

---

[347] *See* letters from Virtu; SIFMA.

[348] *See* letter from SCG.

[349] *See* letter from ISA.

[350] *See*, *e.g.*, letters from CTIA ("The wireless industry is also regulated by the FCC, in several relevant respects . . . In addition to FCC requirements, wireless carriers comply with disclosure obligations under state law, which may require notices to individual consumers and state regulators. Providers are also subject to FCC reporting requirements regarding network outages."); Sen. Portman ("Congress intended that the Cyber Incident Reporting for Critical Infrastructure Act be the primary means for reporting of cyber incidents to the Federal Government, that such reporting be through CISA, and that the required rule occupy the space regarding cyber incident reporting"); SIFMA (stating the proposal "is unwarranted in light of other, existing regulations and the Commission's lack of statutory responsibility for cybersecurity regulation of public companies").

[351] *See* letter from CalPERS. *Accord* letter from Better Markets ("Even in instances where a company discloses relevant cybersecurity incidents, board and management oversights and abilities, and policies and procedures in

comprehensive disclosure of material cyber events exposes investors and the community at large to potential harm."[352]

As the Commission explained in the Proposing Release, Commission staff has observed insufficient and inconsistent cybersecurity disclosure notwithstanding the prior guidance.[353] Here, in response to commenters, we emphasize that the final rules supplement the prior guidance but do not replace it. The final rules are aimed at remedying the lack of material cybersecurity incident disclosure, and the scattered, varying nature of cybersecurity strategy, risk management, and governance disclosure, the need for which some commenters confirmed.[354] The final rules therefore add an affirmative cybersecurity incident disclosure obligation, and they centralize cybersecurity risk management, strategy, and governance disclosure. While we acknowledge commenters who noted the improvements to certain cybersecurity-related disclosures in response to the 2018 Interpretive Release, and we agree there have been improvements in the areas that the guidance touched upon, we note that the guidance does not mandate consistent or comparable public disclosure of material incidents or otherwise address the topics that are the subject of the final rules. And in response to commenters who suggested that other agencies' rules on cybersecurity reporting are sufficient, we note that, unlike the final rules, such rules are not tailored to the informational needs of investors; instead, they focus on the needs of regulators, customers, and individuals whose data have been breached. Accordingly, we believe the final rules are necessary and appropriate in the public interest and

---

a comprehensive manner, the information is scattered throughout various sections of the Form 10-K. While the 2018 guidance adopted by the Commission successfully identified potential disclosure requirements for companies to think about when disclosing cybersecurity risks, governance, and incidents, it did not solve the problem confronting investors who must search various sections of the Form 10-K for the disclosures.").

352 *See* letter from CII.

353 Proposing Release at 16594, 16599, 16603.

354 *See supra* notes 351 and 352.

for the protection of investors, consistent with the Commission's authority.

We also note that the 2018 Interpretive Release remains in place, as it treats a number of topics not covered by the new rules. Those topics include, for instance, incorporating cybersecurity-related information into risk factor disclosure under Regulation S-K Item 105, into management's discussion and analysis under Regulation S-K Item 303, into the description of business disclosure under Regulation S-K Item 101, and, if there is a relevant legal proceeding, into the Regulation S-K Item 103 disclosure.[355] The 2018 Interpretive Release also notes the Commission's expectation that, consistent with Regulation S-X, a company's financial reporting and control systems should be designed 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.[356]

With respect to the Commission's authority to adopt the final rules, some commenters asserted that the Commission does not have the authority to regulate cybersecurity disclosure.[357] These commenters argued that the Proposing Release did not adequately explain which statutory provisions the Commission was relying on to propose the disclosure requirements, that the statutory provisions the Commission did identify do not provide a legal basis to require the proposed disclosures, that the release did not show the requirements were necessary or appropriate to achieve statutory goals, and that the requirements implicate the major questions doctrine and non-delegation principles. Additionally, one commenter stated that "Congress

355 *See* 2018 Interpretive Release.

356 *Id.*

357 *See* letters from International Association of Drilling Contractors; NRF; Virtu.

intended that [CIRCIA] be the primary means for reporting of cyber incidents to the federal government."[358]

We disagree. Disclosure to investors is a central pillar of the Federal securities laws. The Securities Act of 1933 "was designed to provide investors with full disclosure of material information concerning public offerings of securities."[359] In addition, the Securities Exchange Act of 1934 imposes "regular reporting requirements on companies whose stock is listed on national securities exchanges."[360] Together, the provisions of the Federal securities laws mandating release of information to the market—and authorizing the Commission to require additional disclosures—have prompted the Supreme Court to "repeatedly" describe "the fundamental purpose" of the securities laws as substituting "a philosophy of full disclosure for the philosophy of caveat emptor."[361] This bedrock principle of "[d]isclosure, and not paternalistic withholding of accurate information, is the policy chosen and expressed by Congress."[362] Moreover, "[u]nderlying the adoption of extensive disclosure requirements was a

---

358 *See* letter from Sen. Portman. We address this comment in Section II.A.3, *supra*.

359 *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 195 (1976); *accord Pinter v. Dahl*, 486 U.S. 622 (1988) ("[t]he primary purpose of the Securities Act is to protect investors by requiring publication of material information thought necessary to allow them to make informed investment decisions concerning public offerings of securities in interstate commerce").

360 *Ernst & Ernst*, 425 U.S. at 195 (1976); *see also Lawson v. FMR LLC*, 571 U.S. 429, 451 (2014) (referring to the Sarbanes-Oxley Act's "endeavor to 'protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws'" (quoting Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, 745 (2002))).

361 *Lorenzo v. SEC*, 139 S. Ct. 1094, 1103 (2019); *accord Santa Fe Indus. v. Green*, 430 U.S. 462, 477-778 (1977); *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128, 151 (1972); *SEC v. Capital Gains Research Bureau, Inc.*, 375 U.S. 180, 186 (1963).

362 *Basic*, 485 U.S. at 234. Congress also legislated on the core premise that "public information generally affects stock prices," *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 272 (2014), and those prices can significantly affect the economy, 15 U.S.C. 78b(2) and (3).

legislative philosophy: 'There cannot be honest markets without honest publicity. Manipulation and dishonest practices of the market place thrive upon mystery and secrecy.'"[363]

Several provisions of the Federal securities laws empower the Commission to carry out these fundamental Congressional objectives. Under the Securities Act, the Commission has authority to require, in a publicly filed registration statement, that issuers offering and selling securities in the U.S. public capital markets include information specified in Schedule A of the Act, including the general character of the issuer's business, the remuneration paid to its officers and directors, details of its material contracts and certain financial information, as well as "such other information . . . as the Commission may by rules or regulations require as being necessary or appropriate in the public interest or for the protection of investors."[364] In addition, under the Exchange Act, issuers of securities traded on a national securities exchange or that otherwise have total assets and shareholders of record that exceed certain thresholds must register those securities with the Commission by filing a registration statement containing "[s]uch information, in such detail, as to the issuer" in respect of, among other things, "the organization, financial structure and nature of the [issuer's] business" as the Commission by rule or regulation determines to be in the public interest or for the protection of investors.[365] These same issuers must also provide "such information and documents . . . as the Commission shall require to keep reasonably current the information and documents required to be included in or filed with [a] . . .

---

[363] *Basic*, 485 U.S. at 230 (quoting H.R. Rep. No. 73-1383, at 11 (1934)); *accord SEC v. Zandford*, 535 U.S. 813, 819 (2002) ("Among Congress' objectives in passing the [Exchange] Act was 'to insure honest securities markets and thereby promote investor confidence' after the market crash of 1929" (quoting *United States v. O'Hagan*, 521 U.S. 642, 658 (1997))); *Nat'l Res. Def. Council, Inc. v. SEC*, 606 F.2d 1031, 1050 (D.C. Cir. 1979) (the Securities Act and Exchange Act "were passed during an unprecedented economic crisis in which regulation of the securities markets was seen as an urgent national concern," and the Commission "was necessarily given very broad discretion to promulgate rules governing corporate disclosure," which is "evident from the language in the various statutory grants of rulemaking authority").

[364] Securities Act Section 7(a)(1) and Schedule A.

[365] Exchange Act Sections 12(b) and 12(g).

registration statement" as the Commission may prescribe as necessary or appropriate for the proper protection of investors and to insure fair dealing in the security.[366] Separately, these issuers also must disclose "on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer . . . as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest."[367]

These grants of authority are intentionally broad.[368] Congress designed them to give the Commission, which regulates dynamic aspects of a market economy, the power and "flexibility" to address problems of inadequate disclosure as they arose.[369] As the United States Court of Appeals for the District of Columbia Circuit explained, "[r]ather than casting disclosure rules in stone, Congress opted to rely on the discretion and expertise of the SEC for a determination of what types of additional disclosure would be desirable."[370]

The Commission has long relied on the broad authority in these and other statutory provisions[371] to prescribe rules to ensure that the public company disclosure regime provides

---

366 Exchange Act Section 13(a). Other issuers that are required to comply with the reporting requirements of Section 13(a) include those that voluntarily register a class of equity securities under Exchange Act Section 12(g)(1) and, pursuant to Exchange Act 15(d), issuers that file a registration statement under the Securities Act that becomes effective.

367 Exchange Act Section 13(l).

368 *See Natural Resources Defense Council, Inc. v. SEC*, 606 F.2d 1031, 1045 (1979); *see also* H.R. REP. NO. 73-1383, at 6-7 (1934).

369 Courts have routinely applied and interpreted the Commission's disclosure regulations without suggesting that the Commission lacked the authority to promulgate them. *See, e.g., SEC v. Life Partners Holdings, Inc.*, 854 F.3d 765 (5th Cir. 2017) (applying regulations regarding disclosure of risks and revenue recognition); *SEC v. Das*, 723 F.3d 943 (8th Cir. 2013) (applying Regulation S-K provisions regarding related-party transactions and executive compensation); *Panther Partners Inc. v. Ikanos Commc'ns, Inc.*, 681 F.3d 114 (2d Cir. 2012) (applying Item 303 of Regulation S-K, which requires disclosure of management's discussion and analysis of financial condition); *SEC v. Goldfield Deep Mines Co.*, 758 F.2d 459 (9th Cir. 1985) (applying disclosure requirements for certain legal proceedings).

370 *Natural Resources Defense Council, Inc.,* 606 F.2d at 1045.

371 Securities Act Section 19(a); Exchange Act Section 3(b); and Exchange Act Section 23(a).

investors with the information they need to make informed investment and voting decisions, in each case as necessary or appropriate in the public interest or for the protection of investors.[372] Indeed, the Commission's predecessor agency,[373] immediately upon enactment of the Securities Act, relied upon such authority to adopt Form A-1, precursor to today's Form S-1 registration statement, to require disclosure of information including, for example, a list of states where the issuer owned property and was qualified to do business and the length of time the registrant had been engaged in its business—topics that are not specifically enumerated in Schedule A of the Securities Act.[374] Form A-1 also required disclosures related to legal proceedings, though there is no direct corollary in Schedule A.[375]

Consistent with the statutory scheme that Congress enacted, the Commission has continued to amend its disclosure requirements over time in order to respond to marketplace developments and investor needs. Accordingly, over the last 90 years, the Commission has eliminated certain disclosure items and adopted others pursuant to the authority in Sections 7 and 19(a) of the Securities Act and Sections 3(b), 12, 13, 15, and 23(a) of the Exchange Act. Those amendments include the adoption of an integrated disclosure system in 1982, which reconciled

---

372 In considering whether a particular item of disclosure is necessary or appropriate in the public interest or for the protection of investors, the Commission considers both the importance of the information to investors as well as the costs to provide the disclosure. In addition, when engaged in rulemaking that requires it to consider or determine whether an action is necessary or appropriate in the public interest, the Commission also must consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation. *See* Section 2(b) of the Securities Act and Section 3(f) of the Exchange Act.

373 Prior to enactment of the Exchange Act, the Federal Trade Commission was empowered with administration of the Securities Act.

374 Items 3 through 5 of Form A-1; *see* Release No. 33-5 (July 6, 1933) [not published in the Federal Register]. The Commission's disclosure requirements no longer explicitly call for this information.

375 This early requirement called for a statement of all litigation that may materially affect the value of the security to be offered, including a description of the origin, nature, and names of parties to the litigation. Item 17 of Form A-1. The Commission has retained a disclosure requirement related to legal proceedings in both Securities Act registration statements and in Exchange Act registration statements and periodic reports. 17 CFR 229.103.

the various disclosure items under the Securities Act and the Exchange Act and was intended to ensure that "investors and the marketplace have been provided with meaningful, nonduplicative information upon which to base investment decisions."[376]

In keeping with Congressional intent, the Commission's use of its authority has frequently focused on requiring disclosures that will give investors enhanced information about risks facing registrants. For example, in 1980, the Commission adopted Item 303 of Regulation S-K to require registrants to include in registration statements and annual reports a management's discussion and analysis of financial condition ("MD&A"). This discussion is intended to allow investors to understand the registrant's "financial condition, changes in its financial condition and results of operation" through the eyes of management.[377] Item 303 includes a number of specific disclosure items, such as requiring the identification of any known trends or uncertainties that will result in, or that are reasonably likely to result in, a material change to the registrant's liquidity,[378] a material change in the mix and relative cost of the registrant's capital resources,[379] or a material impact on net sales, revenues, or income from continuing operations.[380] Item 303 also requires registrants to "provide such other information

---

376 *See Adoption of Integrated Disclosure System*, Release No. 33-6383 (Mar. 3, 1982) [47 FR 11380 (Mar. 16, 1982)]. Even prior to the adoption of the integrated disclosure system in 1982, the Commission addressed anticipated disclosure issues in particular areas through the use of Guides for the Preparation and Filing of Registration Statements. *See Proposed Revision of Regulation S-K and Guides for the Preparation and Filing of Registration Statements and Reports*, Release No. 33-6276 (Dec. 23, 1980) [46 FR 78 (Jan. 2, 1981)] (discussing the use of Guides); *see also Notice of Adoption of Guide 59 and of Amendments to Guides 5 and 16 of the Guides for Preparation and Filing of Registration Statements Under the Securities Act of 1933*, Release No. 33-5396 (Jun. 1, 1973) (discussing, in response to fuel shortages in 1974, the obligation to disclose any material impact that potential fuel shortages might have and adding a new paragraph relating to disclosure by companies engaged in the gathering, transmission, or distribution of natural gas).

377 *See Management's Discussion and Analysis of Financial Condition and Results of Operations; Certain Investment Company Disclosures*, Release No. 33-6231 (Sept. 2, 1980) [45 FR 63630 (Sept. 25, 1980)]; *see also* 17 CFR 229.303(a).

378 *See* 17 CFR 229.303(b)(1)(i).

379 *See* 17 CFR 229.303(b)(1)(ii)(B).

380 *See* 17 CFR 229.303(b)(2)(ii).

that the registrant believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operation."[381] The Commission developed the MD&A disclosure requirements to supplement and provide context to the financial statement disclosures previously required by the Commission.

A few years later, in 1982, the Commission codified a requirement that dated back to the 1940s for registrants to include a "discussion of the material factors that make an investment in the registrant or offering speculative or risky," commonly referred to as "risk factors."[382] By definition, these disclosures encompass a discussion of risks, or prospective future events or losses, that might affect a registrant or investment. The initial risk factor disclosure item provided examples of possible risk factors, such as the absence of an operating history of the registrant, an absence of profitable operations in recent periods, the nature of the business in which the registrant is engaged or proposes to engage, or the absence of a previous market for the registrant's common equity.[383]

In subsequent years, the Commission expanded both the scope of risks about which registrants must provide disclosures and the granularity of those disclosures. For example, in 1997, the Commission first required registrants to disclose quantitative information about market

---

381 17 CFR 229.303(b).

382 *See Adoption of Integrated Disclosure System*, Release No. 33-6383 (Mar. 3, 1982) [47 FR 11380 (Mar. 16, 1982)] ("Release No. 33-6383") (codifying the risk factor disclosure requirement as Item 503(c) of Regulation S-K); *see also* 17 CFR 229.105(a). Prior to 1982, the Commission stated in guidance that, if the securities to be offered are of a highly speculative nature, the registrant should provide "a carefully organized series of short, concise paragraphs summarizing the principal factors that make the offering speculative." *See* Release No. 33-4666 (Feb. 7, 1964) [29 FR 2490 (Feb. 15, 1964)]. A guideline to disclose a summary of risk factors relating to an offering was first set forth by the Commission in 1968 and included consideration of five factors that may make an offering speculative or risky, including with respect to risks involving "a registrant's business or proposed business." *See* Guide 6, in *Guides for the Preparation and Filing of Registration Statements*, Release No. 33-4936 (Dec. 9, 1968) [33 FR 18617 (Dec. 16, 1968)] ("Release No. 33-4936").

383 *See* Release No. 33-6383.

risk.[384] That market risk disclosure included requirements to present "separate quantitative information . . . to the extent material" for different categories of market risk, such as "interest rate risk, foreign currency exchange rate risk, commodity price risk, and other relevant market risks, such as equity price risk."[385] Under these market risk requirements, registrants must also disclose various metrics such as "value at risk" and "sensitivity analysis disclosures." In addition, registrants must provide certain qualitative disclosures about market risk, to the extent material.[386]

Each of these disclosure items reflects the Commission's long-standing view that understanding the material risks faced by a registrant and how the registrant manages those risks can be just as important to assessing its business operations and financial condition as knowledge about its physical assets or material contracts. Indeed, investors may be unable to assess the value of those assets or contracts adequately without appreciating the material risks to which they are subject.[387]

In addition to risk-focused disclosures, over the decades, the Commission has also required registrants to provide information on a diverse range of topics that emerged as significant to investment or voting decisions, such as the extent of the board's role in the risk

---

[384] *See Disclosure of Accounting Policies for Derivative Financial Instruments and Derivative Commodity Instruments and Disclosure of Quantitative and Qualitative Information About Market Risk Inherent in Derivative Financial Instruments, Other Financial Instruments, and Derivative Commodity Instruments*, Release No. 33-7386 (Jan. 31, 1997) [62 FR 6044 (Feb. 10, 1997)] ("Release No. 33-7386") ("In light of those losses and the substantial growth in the use of market risk sensitive instruments, the adequacy of existing disclosures about market risk emerged as an important financial reporting issue."); *see also* 17 CFR 229.305.

[385] 17 CFR 229.305(a)(1).

[386] *See* 17 CFR 229.305(b).

[387] As early as the 1940s, the Commission issued stop order proceedings under Section 8(d) of the Securities Act in which the Commission suspended the effectiveness of previously filed registration statements due, in part, to inadequate disclosure about speculative aspects of the registrant's business. *See* In the Matter of Doman Helicopters, Inc., 41 S.E.C. 431 (Mar. 27, 1963); In the Matter of Universal Camera Corp., 19 S.E.C. 648 (June 28, 1945)); *see also* Release No. 33-4936.

oversight of the registrant,[388] the effectiveness of a registrant's disclosure controls and procedures,[389] related-party transactions,[390] corporate governance,[391] and compensation discussion and analysis,[392] among many other topics, including on topics related to particular industries,[393] offering structures,[394] and types of transactions.[395] In all these instances, the Commission's exercise of its authority was guided by the baseline of the specific disclosures articulated by Congress. But, as Congress expressly authorized,[396] the Commission's exercise of its disclosure authority has not been narrowly limited to those statutorily prescribed disclosures—instead, it has been informed by both those disclosures and the need to protect investors.[397] Many of these disclosures have since become essential elements of the public company reporting regime that Congress established.

To ensure the transparency that Congress intended when it authorized the Commission to promulgate disclosure regulations in the public interest or to protect investors,[398] the Commission's regulations must—as they have over time—be updated to account for changing

---

388 *See* 17 CFR 229.407.

389 *See* 17 CFR 229.307.

390 17 CFR 229.404.

391 17 CFR 229.407.

392 17 CFR 229.402.

393 *See* 17 CFR 229.1200-1208 (Disclosure by Registrants Engaged in Oil and Gas Activities); 17 CFR 1300-1305 (Disclosure by Registrants Engaged in Mining Operations); 17 CFR 1400-1406 (Disclosure by Bank and Savings and Loan Registrants).

394 *See* 17 CFR Subpart 1100 (Asset-Backed Securities).

395 *See* 17 CFR subpart 900 (Roll-Up Transactions); 17 CFR 229.1000-1016 (Mergers and Acquisitions).

396 *See supra* notes 364 to 366 and accompanying text.

397 For example, Item 303(b)(2) of Regulation S-K calls for information well beyond the basic profit and loss statement specified in Schedule A by requiring issuers to disclose any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income—and the extent to which income was so affected—so that investors can better understand the reported results of operations.

398 *See supra* notes 368 to 370 and accompanying text.

market conditions, new technologies, new transaction structures, and emergent risks. In this regard, we disagree with one commenter's assertion that the Commission's disclosure authority is "limited to specific types of information closely related to the disclosing company's value and financial condition."[399] The commenter misstates the scope and nature of the Commission's authority. There is a wealth of information about a company apart from that which appears in the financial statements that is related to a company's value and financial condition, including the material risks (cybersecurity and otherwise) a company faces. Nor did Congress dictate that the Commission limit disclosures only to information that is "closely related" to a company's "value and financial condition." By also empowering the Commission to require "such other information . . . as the Commission may by rules or regulations require as being necessary or appropriate in the public interest or for the protection of investors,"[400] Congress recognized that there is information that is vital for investors to understand in making informed investment decisions but does not directly relate to a company's value and financial condition.[401]

The narrow reading of the Commission's authority advocated by the commenter would foreclose many of these longstanding elements of disclosure that market participants have come to rely upon for investor protection and fair dealing of securities.[402] Moreover, Congress itself has amended, or required the Commission to amend, the Federal securities laws many times. But Congress has not restricted the Commission's disclosure authority; rather, Congress has typically sought to further expand and supplement that authority with additional mandated disclosures.

---

399 *See* letter from NRF.

400 Securities Act Section 7(a).

401 For example, Schedule A calls for information regarding, among other things: the names of the directors or persons performing similar functions, the disclosure of owners of record of more than 10% of any class of stock of an issuer; commissions paid to underwriters; the renumeration paid to directors and certain officers; and information about certain material contracts.

402 *See* letter from NRF.

We also reject the commenter's suggestion that the final rules are an attempt to "usurp the undelegated role of maintaining cyber safety in America."[403] The final rules are indifferent as to whether and to what degree a registrant may have identified and chosen to manage a cybersecurity risk. Rather, the final rules reflect the reality, as acknowledged by the same commenter, that "[c]ybersecurity is . . . an area of growing importance to companies across the world."[404] When those companies seek to raise capital from investors in U.S. public markets, we believe it is appropriate that they share information about whether and, if so, how they are managing material cybersecurity risks so that investors can make informed investment and voting decisions consistent with their risk tolerance and investment objectives.

Finally, with respect to the commenter's contention that a broad reading of the Commission's disclosure authority could raise separation of powers concerns,[405] we note that a statutory delegation is constitutional as long as Congress lays down by legislative act an intelligible principle to which the person or body authorized to exercise the delegated authority is directed to conform.[406] In this instance, Congress has required that any new disclosure requirements be "necessary or appropriate in the public interest or for the protection of investors,"[407] which has guided the Commission's rulemaking authority for nearly a century. We therefore believe that the final rules are fully consistent with constitutional principles regarding separation of powers.

---

403 *Id*.

404 *Id*.

405 *Id*.

406 *Gundy v. U.S.*, 139 S. Ct. 2116, 2123 (plurality op.).

407 *See* Securities Act Section 19(a) and Exchange Act Section 23(a); *accord Nat'l Res. Def. Council*, 606 F.2d at 1045, 1050–52.

I. Compliance Dates

The final rules are effective September 5, 2023. With respect to Item 106 of Regulation S-K and item 16K of Form 20-F, all registrants must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the incident disclosure requirements in Item 1.05 of Form 8-K and in Form 6-K, all registrants other than smaller reporting companies must begin complying on December 18, 2023. As discussed above, smaller reporting companies are being given an additional 180 days from the non-smaller reporting company compliance date before they must begin complying with Item 1.05 of Form 8-K, on June 15, 2024.

With respect to compliance with the structured data requirements, as noted above, all registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after the initial compliance date for any issuer for the related disclosure requirement. Specifically:

- For Item 106 of Regulation S-K and item 16K of Form 20-F, all registrants must begin tagging responsive disclosure in Inline XBRL beginning with annual reports for fiscal years ending on or after December 15, 2024; and
- For Item 1.05 of Form 8-K and Form 6-K all registrants must begin tagging responsive disclosure in Inline XBRL beginning on December 18, 2024.

III. OTHER MATTERS

If any of the provisions of these rules, or the application thereof to any person or circumstance, is held to be invalid, such invalidity shall not affect other provisions or application of such provisions to other persons or circumstances that can be given effect without the invalid provision or application.

Pursuant to the Congressional Review Act, the Office of Information and Regulatory Affairs has designated these rules as not a "major rule," as defined by 5 U.S.C. 804(2).

IV. ECONOMIC ANALYSIS

A. Introduction

We are mindful of the costs imposed by, and the benefits to be obtained from, our rules. Section 2(b) of the Securities Act[408] and Section 3(f) of the Exchange Act[409] direct 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[410] 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. The discussion below addresses the economic effects of the final rules, including the likely benefits and costs, as well as the likely effects on efficiency, competition, and capital formation.

Where possible, we have attempted to quantify the benefits, costs, and effects on efficiency, competition, and capital formation expected to result from the final rules. In some cases, however, we are unable to quantify the potential economic effects because we lack information necessary to provide a reasonable estimate. For example, we lack the data to estimate any potential decrease in mispricing that might result from the rule, because we do not know how registrants' disclosures of cybersecurity risk and governance will change or which

---

408 15 U.S.C. 77b(b).

409 15 U.S.C. 78c(f).

410 15 U.S.C. 78w(a)(2).

cybersecurity incidents that would go undisclosed under the current guidance will be disclosed under the final rules. Where we are unable to quantify the economic effects of the final rules, we provide a qualitative assessment of the effects, and of the impacts of the final rule on efficiency, competition, and capital formation. To the extent applicable, the views of commenters relevant to our analysis of the economic effects, costs, and benefits of these rules are included in the discussion below.

While cybersecurity incident disclosure has become more frequent since the issuance of the 2011 Staff Guidance and 2018 Interpretive Release, there is concern that variation persists in the timing, content, and format of registrants' existing cybersecurity disclosure, and that such variation may harm investors (as further discussed below).[411] When disclosures about cybersecurity breaches are made, they may not be timely or consistent. Because of the lack of consistency in when and how companies currently disclose incidents, it is difficult to assess quantitatively the timeliness of disclosures under current practices. According to Audit Analytics data, in 2021, it took on average of 42 days for companies to discover breaches, and then it took an average of 80 days and a median of 56 days for companies to disclose a breach after its discovery.[412] These data do not tell us when disclosure occurs relative to companies' materiality determinations. That said, the report notes that some breaches were disclosed for the first time to investors in periodic reports, the timing of which are unrelated to the timing of the

---

411 *See supra* Section I. *See also supra* note 18 and accompanying text; Eli Amir, Shai Levi, & Tsafrir Livne, *Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets*, 23 REV. ACCT. STUD. 1177 (2018).

412 AUDIT ANALYTICS, *Trends in Cybersecurity Breaches* (Apr. 2022), *available at https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_April_2022.pdf* ("Audit Analytics") (looking specifically at disclosures by companies with SEC filing requirements and 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 and reputational costs that can directly impact financial performance, such as reduced revenue due to lost sales.").

incident or the company's assessment of the materiality of the incident. This implies at least some cybersecurity incident disclosures were not timely with respect to determination of materiality. Because cybersecurity incidents can significantly affect registrants' stock prices, delayed disclosure results in mispricing of securities, harming investors.[413] Incident disclosure practices, with respect to both location and content, currently vary across registrants. For example, some registrants disclose incidents through Form 10-K, others Form 8-K, and still others on a company website, or in a press release. Some disclosures do not discuss whether the cybersecurity incident had material impact on the company.[414] Additionally, evidence suggests registrants may be underreporting cybersecurity incidents.[415] More timely, informative, and standardized disclosure of material cybersecurity incidents may help investors to assess an incident's impact better.

While disclosures about cybersecurity risk management, strategy, and governance have been increasing at least since the issuance of the 2018 Interpretive Release, they are not currently provided by all registrants. Despite the increasing prevalence of references to cybersecurity risks in disclosures, however, registrants do not consistently or uniformly disclose information related to cybersecurity risk management, strategy, and governance.[416] Registrants currently make such disclosures in varying sections of a company'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 sometimes include them with other

---

413 *See* Shinichi Kamiya, et al., *Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms*, 139 J. FIN. ECON. 721 (2021).

414 Based on staff analysis of the current and periodic reports in 2022 for companies identified by having been affected by a cybersecurity incident.

415 *See* BITDEFENDER, *supra* note 18 and accompanying text.

416 *See supra* Section II.C.1.b. and c.; *see also* letter from Better Markets.

unrelated disclosures.[417] One commenter noted that current disclosure is "piecemeal" in nature and that the varying content and placement make it difficult for investors and other market participants to locate and understand the cybersecurity risks that registrants face and their preparedness for an attack, and to make comparisons across registrants.[418]

As we discuss in more detail below, some commenters supported the proposed rule. Specifically, one commenter noted that markets responded negatively to delayed cybersecurity disclosures, suggesting that timeliness in disclosing incidents is valuable to investors.[419] Further, some academic commenters submitted papers that they authored finding that evidence suggests that companies experiencing data breaches subsequently experience higher borrowing costs.[420] On the other hand, other commenters contended that the proposed rules would hinder capital formation, particularly for small registrants,[421] or that a more cost-effective alternative to the proposed rules would be to look to existing rules to elicit relevant disclosures, as articulated by the 2011 Staff Guidance and the 2018 Interpretive Release.[422] Several commenters pointed out that the proposed disclosures on cybersecurity risk management, strategy, and governance might be overly prescriptive and would potentially provide a roadmap for threat actors, and that these rules could increase, not decrease costs.[423] In response to those comments, these provisions have

---

417 *See* Proposing Release at 16606 (Table 1. Incidence of Cybersecurity-Related Disclosures by 10-K Location).

418 *See* letter from Better Markets.

419 *See* letter from Prof. Choudhary.

420 *See* letters from Profs. Huang & Wang; Prof. Sheneman.

421 *See* letter from BIO.

422 *See* letter from NRF.

423 *See* letters from ABA; ACLI; APCIA; BIO; BPI et al.; Business Roundtable; Chamber; CSA; CTIA; EIC; Enbridge; FAH; Federated Hermes; GPA; ITI; ISA; Nareit; NAM; NMHC; NRA; NRF; SIFMA; Sen. Portman; TechNet; TransUnion; USTelecom; Virtu.

been modified in the final rule, which should reduce the perceived risk of providing a roadmap for threat actors compared with the proposal.

B. Economic Baseline

1. Current Regulatory Framework

To assess the economic impact of the final rules, the Commission is using as its baseline the existing regulatory framework and market practice for cybersecurity disclosure. Although a number of Federal and State rules and regulations obligate registrants to disclose cybersecurity risks and incidents in certain circumstances, the Commission's regulations currently do not explicitly address cybersecurity.[424]

As noted in the Proposing Release, cybersecurity threats and incidents continue to increase in prevalence and seriousness, posing an ongoing and escalating risk to public registrants, investors, and other market participants.[425] The number of reported breaches disclosed by public companies has increased almost 600 percent over the last decade, from 28 in 2011 to 131 in 2020 and 188 in 2021.[426] Although estimating the total cost of cybersecurity incidents is difficult, as many events may be unreported, some estimates put the economy-wide total costs as high as trillions of dollars per year in the U.S. alone.[427] The U.S. Council of Economic Advisers estimated that in 2016 the total cost of cybersecurity incidents was between

---

424 *See* Proposing Release at 16593-94 for a detailed discussion of the existing regulatory framework.

425 Unless otherwise noted, when we discuss the economic effects of the final rules on "other market participants," we mean those market participants that typically provide services for investors and who rely on the information in companies' filings (such as financial analysts, investment advisers, and portfolio managers).

426 Audit Analytics, *supra* note 412.

427 See CYBERSECURITY & INFRASTRUCTURE SEC. 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* (based on a literature review of publications discussing incidents that occurred in the United States or to U.S.-based companies).

$57 billion and $109 billion, or between 0.31 and 0.58 percent of U.S. GDP in that year.[428] A more recent estimate suggests the average cost of a data breach in the U.S. is $9.44 million.[429] Executives, boards of directors, and investors remain focused on the emerging risk of cybersecurity. A 2022 survey of bank Chief Risk Officers found that they identified managing cybersecurity risk as the top strategic risk.[430] In 2022, a survey of audit committee members again identified cybersecurity as a top area of focus in the coming year.[431]

In 2011, the Division of Corporation Finance issued interpretive guidance providing the Division's views concerning operating registrants' disclosure obligations relating to cybersecurity risks and incidents.[432] This 2011 Staff Guidance provided an overview of existing disclosure obligations that may require a discussion of cybersecurity risks and cybersecurity incidents, along with examples of potential disclosures.[433] 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.[434] In the 2018

---

428 COUNCIL OF ECON. ADVISERS, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Feb. 2018), *available at https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/* (estimating total costs, rather than costs of only known and disclosed incidents).

429 Ponemon Institute & IBM Security, *Cost of a Data Breach Report 2022* (July 2022), *available at https://www.ibm.com/downloads/cas/3R8N1DZJ* (estimating based on analysis of 550 organizations impacted by data breaches that occurred between Mar. 2021 and Mar. 2022).

430 EY AND INSTITUTE OF INTERNATIONAL FINANCE, *12th Annual EY/IIF Global Bank Risk Management Survey*, at 14 (2022), *available at https://www.iif.com/portals/0/Files/content/32370132_ey-iif_global_bank_risk_management_survey_2022_final.pdf* (stating 58% of surveyed banks' Chief Risk Officers cite "inability to manage cybersecurity risk" as the top strategic risk). *See also* EY, *EY CEO Imperative Study* (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*.

431 CENTER FOR AUDIT QUAL. & DELOITTE, *Audit Committee Practices Report: Priorities and Committee Composition* (Jan. 2023) *available at https://www.thecaq.org/audit-committee-practices-report-2023/*. *See also* CENTER FOR AUDIT QUAL. & DELOITTE, *Audit Committee Practices Report: Common Threads Across Audit Committees* (Jan. 2022), *available at https://www.thecaq.org/2022-ac-practices-report/*.

432 *See* 2011 Staff Guidance.

433 *Id*.

434 *See* 2018 Interpretive Release.

Interpretive Release, the Commission reiterated that registrants must 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.[435] Additionally, the 2018 Interpretive Release encouraged registrants to continue to use current reports (Form 8-K or Form 6-K) to disclose material information promptly, including disclosure pertaining to cybersecurity matters.[436] Further, the 2018 Interpretive Release noted that to the extent cybersecurity risks are material to a registrant's business, the Commission believes that the required disclosure of the registrant's risk oversight should include the nature of the board's role in overseeing the management of that cybersecurity risk.[437] The 2018 Interpretive Release also stated that a registrant's controls and procedures should enable it to, among other things, identify cybersecurity risks and incidents and make timely disclosures regarding such risks and incidents.[438] 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.[439]

In keeping with existing obligations, companies are increasingly acknowledging cybersecurity risks in their disclosures. One analysis of disclosures made by Fortune 100 companies that filed 10-Ks and proxy statements found 95 percent of those companies disclosed a focus on cybersecurity risk in the risk oversight section of their proxy statements filed in the

---

435 *Id.* at 8168-8170.

436 *Id.* at 8168.

437 *Id.* at 8170.

438 *Id.* at 8171.

439 *Id.* at 8171-8172.

period ending in May 2022, up from 89 percent of filings in 2020 and 76 percent in 2018.[440] Disclosures of efforts to mitigate cybersecurity risk were found in 99 percent of proxy statements or Forms 10-K, up from 93 percent in 2020 and 85 percent in 2018.[441] The Fortune 100 list is composed of the highest-revenue companies in the United States. As discussed later in this economic analysis, we observed the overall rate of disclosure across not just the largest, but all filers, approximately 8,400, to be approximately 73 percent.[442] Further, one commenter noted that current disclosures are "scattered and unpredictable" rather than "uniform," which "diminishes their effectiveness," and so the final rule should improve investors' ability to find and compare disclosures.[443]

Registrants currently are and may continue to be subject to other cybersecurity incident disclosure requirements developed by various industry regulators and contractual counterparties. As discussed in Section II, CIRCIA was passed in March 2022 and requires CISA to develop and issue regulations on cybersecurity reporting. As set forth in CIRCIA, once those regulations are adopted, covered entities will have 72 hours to report covered cybersecurity incidents to CISA and will also be required to report a ransom payment as the result of a ransomware attack within 24 hours of the payment being made.[444] In addition, Federal contractors may be required to monitor and report cybersecurity incidents and breaches or face liability under the False Claims

---

440 See EY CTR FOR BD MATTERS, *How Cyber Governance and Disclosures are Closing the Gaps in 2022* (Aug. 2022), *available at https://www.ey.com/en_us/board-matters/how-cyber-governance-and-disclosures-are-closing-the-gaps-in-2022*.

441 *Id*.

442 *See infra* note 456 (describing textual analysis) and accompanying text.

443 *See* letter from Better Markets. Although uniformity should improve investors' ability to find and compare disclosures, within that structure the final rule allows customization to capture complexity and avoid unnecessarily simplifying issues for the sake of standardization.

444 6 U.S.C. 681b. *See also supra* notes 21 to 23 and accompanying text.

Act.[445] An FCC rule directs covered telecommunications providers on how and when to disclose breaches of certain customer data.[446] HIPAA requires covered entities and their business associates to provide notification following a breach of unsecured protected health information.[447] Similar rules require vendors of personal health records and related entities to report data breaches to affected individuals and the FTC.[448] All 50 states have data breach laws that require businesses to notify individuals of security breaches involving their personally identifiable information.[449] There are other rules that registrants must follow in international jurisdictions. For example, in the European Union, the General Data Protection Regulation mandates disclosure of cybersecurity breaches.[450]

These other cybersecurity incident disclosure requirements may cover some of the material incidents that registrants will need to disclose under the final rules. However, not all registrants are subject to each of these other incident disclosure requirements and the timeliness and public reporting elements of these requirements vary, making it difficult for investors and

---

445 See DEP'T OF JUSTICE, OFFICE OF PUB. 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").

446 *See* 47 CFR 64.2011; *see also supra* Section II.A.3.

447 *See* 45 CFR 164.400 through 414 (Notification in the Case of Breach of Unsecured Protected Health Information).

448 *See* 16 CFR 318 (Health Breach Notification Rule).

449 Note that there are carve-outs to these rules, and not every company may fall under any particular rule. *See* NAT'L CONFERENCE OF STATE LEGISLATURES, *Security Breach Notification Laws* (updated Jan. 17, 2022), *available at https://www.ncsl.org/technology-and-communication/security-breach-notification-laws*.

450 *See* Regulation (EU) 2016/679, of the European Parliament and the Council of 27 Apr. 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").

other market participants to be alerted to the breaches and to gain an adequate understanding of the impact of such incidents on a registrant.

Some registrants are also subject to other mandates regarding cybersecurity risk management, strategy, and governance. For instance, government contractors may be subject to the Federal Information Security Modernization Act, and use the NIST framework to manage information and privacy risks.[451] Certain financial institutions may be subject to the FTC's Standards for Safeguarding Customer Information Rule, requiring an information security program, including a qualified individual to oversee the security program, and the provision of periodic reports on the cybersecurity program to a company's board of directors or equivalent governing body.[452] Under HIPAA regulations, covered entities are subject to rules that require protection against reasonably anticipated threats to electronic protected health information.[453] International jurisdictions also have cybersecurity risk mitigation measures and governance requirements (see, for example, the GDPR).[454] These rules and regulations provide varying standards and requirements for disclosing cybersecurity risk management, strategy, and governance, and may not provide investors with public or clear and comparable disclosure regarding how a particular registrant manages its cybersecurity risk profile.

2. Affected Parties

The parties that are likely to be affected by the final rules include investors, registrants, other market participants that use the information provided in company filings (such as financial

---

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

452 *See* 16 CFR 314.

453 *See* 45 CFR 164 (Security and Privacy); *see also supra* Section II.A.3.

454 *See, e.g.,* GDPR, arts. 32 (Security of processing), 37 (Designation of the data protection officer).

analysts, investment advisers, and portfolio managers), and external stakeholders such as consumers and other companies in the same industry as affected companies.

We expect the final rules to affect all registrants with relevant disclosure obligations on Forms 10-K, 20-F, 8-K, or 6-K. This includes (1) approximately 7,300 operating companies filing on domestic forms (of which, approximately 120 are business development companies) and (2) 1,174 FPIs filing on foreign forms, based on all companies that filed such forms or an amendment thereto during calendar year 2022.[455] Our textual analysis[456] of all calendar year 2022 Form 10-K filings and amendments reveals that approximately 73 percent of domestic filers made some kind of cybersecurity-related disclosures, whether of incidents, risk, or governance.

We also analyzed calendar year 2022 Form 8-K and Form 6-K filings. There were 71,505 Form 8-K filings in 2022, involving 7,416 filers, out of which 35 filings reported material cybersecurity incidents.[457] Similarly, there were 27,296 Form 6-K filings in 2022, involving 1,161 filers, out of which 22 filings reported material cybersecurity incidents.

C. Benefits and Costs of the Final Rules

The final rules will benefit investors, registrants, and other market participants, such as financial analysts, investment advisers, and portfolio managers, 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

---

[455] Estimates of affected companies here are based on the number of unique CIKs with at least one periodic report, current report, or an amendment to one of the two filed in calendar year 2022.

[456] In performing this analysis, staff executed computer program-based keyword (and combination of key words) searches. This analysis covered 8,405 Forms 10-K and 10-K/A available in Intelligize (a division of RELX Inc.) filed in calendar year 2022 by 7,486 companies as identified by unique CIK.

[457] The number of filers in our sample is larger than the number of estimated affected parties because, among other reasons, it includes 8-K filings by companies that have not yet filed their first annual report.

asymmetry in the market. The final rules also will entail costs. A discussion of the anticipated economic costs and benefits of the final rules is set forth in more detail below. We first discuss benefits, including benefits to investors and other market participants. We subsequently discuss costs, including the cost of compliance with the final rules. We conclude with a discussion of indirect economic effects on investors, external stakeholders such as consumers, and companies in the same industry with registrants subject to this rule, or those facing similar cybersecurity threats.

1. Benefits

Existing shareholders, and those seeking to purchase shares in registrants subject to the final rules, will be the main beneficiaries of the enhanced disclosure of both cybersecurity incidents and cybersecurity risk management, strategy, and governance as a result of the final rules. Specifically, investors will benefit because: (1) more informative and timely disclosure will improve investor decision-making by allowing investors to better understand a registrant's material cybersecurity incidents, material cybersecurity risks, and ability to manage such risks, reducing information asymmetry and the mispricing of securities in the market; and (2) more uniform and comparable disclosures will 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, will also benefit.

a. More Timely and Informative Disclosure

The final rules provide more timely and informative disclosures, relative to the current disclosure environment, which will allow investors to better understand registrants' cybersecurity incidents, risks, and ability to manage such risks as well as reduce mispricing of

securities in the market. Timeliness benefits to investors will result from the requirement to disclose cybersecurity incidents within four business days of determining an incident was material, as well as the requirement to amend the disclosure to reflect material changes. Information benefits to investors will result from the disclosure of both (1) cybersecurity incidents and (2) cybersecurity risk management, strategy, and governance. Together, the timeliness and information benefits created by the final rules will reduce market mispricing and information asymmetry and potentially lower firms' cost of capital.

We anticipate Item 1.05, governing cybersecurity incident disclosure on Form 8-K, will lead to more timely disclosure to investors.[458] Currently, there is not a specific requirement for a registrant to disclose a cybersecurity incident to investors in a timely manner after its discovery and determination of material impact.[459] Item 1.05's requirement to disclose a material cybersecurity incident on Form 8-K within four business days after determining the incident is material will improve the overall timeliness of the disclosure offered to investors—disclosure that is relevant to the valuation of registrants' securities. It is well-documented in the academic literature that the market reacts negatively to announcements of cybersecurity incidents. For example, one study finds a statistically significant mean cumulative abnormal return of -0.84 percent in the three days following cyberattack announcements, which, according to the study, translates into an average value loss of $495 million per attack.[460] One commenter argued that

---

458 For foreign issuers, the disclosure is made via Form 6-K.

459 *See supra* Sections I and IV.B.1.

460 *See* Shinichi Kamiya, et al., *supra* note 413, at 719-749. *See also* Lawrence A. Gordon, Martin P. Loeb, & 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"); Georgios Spanos & 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 companies). *But see* Katherine Campbell, et al., *The Economic*

the magnitude of stock market reaction to cybersecurity incidents from this study would not be considered significant by market participants, stating that "if a stock had a historical standard deviation of 1 percent and moved 0.8 percent on news, most market participants would suggest that the news was either not significant or the market had priced in that news so the reaction was muted."[461] We note, however, that a cumulative abnormal return (CAR) of -0.84 percent refers not to the total return but to the return relative to how stocks in similar industries and with similar risk profiles moved; thus, indeed, a statistically significantly negative CAR represents a meaningful reaction and change to how the stock price would have moved that day absent the announcement of the cybersecurity incident. By allowing investors to make decisions based on more current, material, information, Item 1.05 will reduce mispricing of securities and information asymmetry in the market.

Information asymmetries due to timing could also be exploited by the malicious actors who caused a cybersecurity incident, those who could access and trade on material information stolen during a cybersecurity incident, or those who learn about the incident before public disclosure, causing further harm to investors who trade unknowingly against those with inside information.[462] Malicious actors may trade ahead of an announcement of a data breach that they

---

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").

461 *See* letter from BIO.

462 *See* Joshua Mitts & 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.").

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 provide incentives for malicious actors to "create" more incidents and proprietary information to trade on, further harming the shareholders of impacted companies.[463] Employees or related third-party vendors of a company experiencing a cybersecurity incident may also learn of the incident and trade against investors in the absence of disclosure. More timely disclosure as a result of Item 1.05 will reduce mispricing by reducing windows of information asymmetry in connection with a material cybersecurity incident, thereby reducing opportunities to exploit the mispricing, enhancing investor protection.

A commenter noted that there is risk the rule could, under certain conditions, aid stock manipulation efforts by malicious actors, offsetting these benefits.[464] One commenter suggested that mandated disclosure timing could make public cybersecurity incident disclosure dates more predictable, and thus trading strategies based on the accompanying negative stock price reaction more consistent, to the extent malicious actors can monitor or control discovery of breaches they cause and correctly anticipate materiality determination timing. Their ability to do this is unclear, but we note that if the final rules increase the precision of strategies by attackers that involve shorting the stock of their targets, that would reduce the benefit of the final rules.

Item 1.05 allows registrants to delay filing for up to 30 days if the Attorney General determines that the incident disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. The delay may be extended

---

[463] *Id.*

[464] *See* letter from ISA.

up to an additional 30 days if the Attorney General determines disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order. These delay periods and possible exemptive relief would curb the timeliness benefits discussed above but would reduce the costs of premature disclosure such as alerting malicious actors targeting critical infrastructure that their activities have been discovered.

By requiring all material cybersecurity incidents to be disclosed, Item 1.05 will also provide investors more informative disclosure by increasing material cybersecurity incident disclosure.[465] There are currently reasons that registrants do not disclose cybersecurity incidents. For example, a registrant's managers may be reluctant to release information that they expect or anticipate will cause their stock price to suffer.[466] Thus an agency problem prevents investors from receiving this useful information. In addition, registrants may consider only the benefits and costs that accrue to them when deciding whether to disclose an incident. As discussed in Section IV.C.3, incident disclosure can create indirect economic effects that accrue to parties other than the company itself. Companies focused on direct economic benefits, however, may not factor in this full range of effects resulting from disclosing cybersecurity incidents, resulting

[465] *See* Amir, Levi, & Levine, *supra* note 411.

[466] *See, e.g.,* Kamiya, et al., *supra* note 413, at 719-749.

in less reporting and less information released to the market. The mandatory disclosure in Item 1.05 should thus lead to more incidents being disclosed, reducing mispricing of securities and information asymmetry in the market as stock prices will more accurately reflect registrants having experienced a cybersecurity incident.

Item 1.05 will also improve the informativeness of the content of cybersecurity incident disclosures. In 2022, when registrants filed a Form 8-K to report an incident, the Form 8-K did not necessarily state whether the incident was material, and in some cases, the Form 8-K stated that the incident was immaterial.[467] Item 1.05 will require registrants to describe in an 8-K filing the material aspects of the nature, scope, and timing of a material cybersecurity incident and the material impact or reasonably likely material impact on the registrant, including on its financial condition and results of operations. The disclosure must also identify any information called for in Item 1.05(a) that is not determined or is unavailable at the time of the required filing. Registrants will then need to disclose this information in a Form 8-K amendment containing such information within four business days after the information is determined or becomes available. Item 1.05 is thus expected to elicit more pertinent information to aid investor decision-making. Additionally, the materiality requirement should minimize immaterial incident disclosure that might divert investor attention, which should reduce mispricing of securities. Numerous commenters on the Proposing Release agreed that more informative incident disclosure would be useful for investors.[468]

Regulation S-K Items 106(b) and (c) of the final rules provide further benefits by requiring registrants to disclose, in their annual reports on Form 10-K, information about their

[467] Based on staff analysis of the 10,941 current and periodic reports in 2022 for companies available in Intelligize and identified as having been affected by a cybersecurity incident using a keyword search.

[468] *See, e.g.*, letters from Better Markets; CalPERS; PWC; Prof. Perullo.

cybersecurity risk management, strategy, and governance. The final rules require disclosure regarding a registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as disclosure of the registrant's board of directors' oversight of risks from cybersecurity threats and management's role in assessing and managing material risks from cybersecurity threats.[469] There are currently no disclosure requirements on Forms 10-K or 10-Q that explicitly refer to cybersecurity risks or governance, and thus Item 106 will benefit investors by eliciting relevant information about how registrants are managing their material cybersecurity risks.

One commenter took issue with the usefulness of the proposed disclosures, arguing, for example, that the particular requirement to disclose whether a registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program was unnecessary because there was no evidence that such third parties improved a registrant's cyber risk management, and some companies have internal cybersecurity risk management capabilities.[470] Some, however, have noted that the use of independent third-party advisors may be "vital to enhancing cyber resiliency" by validating that the risk management program is meeting its objectives.[471] As discussed in Section II.C.1.c., it may be important for investors to know a registrant's level of in-house versus outsourced cybersecurity capacity. Another commenter suggested that the requirement to disclose governance and risk management practices would be of limited value to investors, while being administratively burdensome.[472]

---

469 *See supra* Sections II.B and C. For foreign issuers, the disclosure is made via Form 20-F.

470 *See* letter from NRF.

471 *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/*.

472 *See* letter from SIMFA.

Other commenters said that the required disclosures about cybersecurity governance and risk management were too granular to be useful and suggested that the specific disclosures be replaced with a more high-level explanation of management's and the board's roles in cybersecurity risk management and governance.[473] One such commenter stated that the proposed disclosures would create pressures to provide boilerplate responses to the specific items that would need to be disclosed instead of providing a robust discussion of the way a registrant would manage cybersecurity risk management and governance.[474] Another commenter stated that granular disclosures "may result in overly detailed filings that have little utility to investors."[475] These commenters suggested that the specific disclosures should be replaced with a more high-level explanation of management's and the board's roles in cybersecurity risk management and governance.

In response to these comments, the Commission is not adopting certain proposed disclosure requirements, such as disclosure of whether the registrant has a designated chief information security officer. However, Items 106(b) and (c) still require risk, strategy and governance disclosures as we continue to believe disclosures of cybersecurity risk oversight and processes, as well as management's role and relevant expertise, are important to investors.

Improved timeliness and informativeness of cybersecurity disclosures may provide further benefit by lowering companies' cost of capital.[476] As detailed above, the final rules

---

473 *See* letters from ABA; AGA/INGAA; EEI; Nareit; NYSE.

474 *See* letter from ABA.

475 *See* letter from NYSE.

476 *See* Leuz & Verrecchia*, The Economic Consequences of Increased Disclosure*, 38 J. ACCT. RES. 91 (2000) ("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

should reduce information asymmetry and mispricing of securities. In an asymmetric information environment, investors are less willing to hold shares, reducing liquidity. Registrants may respond by issuing shares at a discount, increasing their cost of capital. By providing more and more credible disclosure, however, companies can reduce the risk of adverse selection faced by investors and the discount they demand, ultimately increasing liquidity and decreasing the company's cost of capital.[477] Investors benefit when the companies they are invested in enjoy higher liquidity. Item 1.05 enables companies to provide more credible disclosure because currently, investors do not know whether an absence of incident disclosure means no incidents have occurred, or one has but the company has not yet chosen to reveal it. By requiring all material incidents to be reported, Item 1.05 supplies investors greater assurance that, indeed, barring extraordinary circumstances, no disclosure means the company has not been aware for more than four business days of a material incident having occurred. Similarly, Item

---

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]).").

[477] *See* Douglas W. Diamond & 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 company's cost of capital through increased liquidity). *See also* Christian Leuz & 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 companies); *see also* Christian Leuz & 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). Although disclosure could be beneficial for the company, several conditions must be met for companies to voluntarily disclose all their private information. *See* Anne Beyer, et al., *The Financial Reporting Environment: Review Of The Recent Literature*, 50 J. ACCT. & ECON. 296, 296-343 (2010) (discussing conditions under which companies voluntarily disclose all their private information, and these conditions include "(1) disclosures are costless; (2) investors know that companies have, in fact, private information; (3) all investors interpret the companies' disclosure in the same way and companies know how investors will interpret that disclosure; (4) managers want to maximize their companies' share prices; (5) companies can credibly disclose their private information; and (6) companies cannot commit ex-ante to a specific disclosure policy"). Increased reporting could also help determine the effect of investment on company value. *See* Lawrence A. Gordon, et al., *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").

106 should also generate more credible disclosure. Currently, voluntary cybersecurity risk management, strategy, and governance disclosures lack standardization and consistency, reducing their comparability and usefulness for investors. Without set topics that must be addressed, companies may disclose only the strongest aspects of their cybersecurity processes, if they disclose at all. By clarifying what registrants must disclose with respect to their cybersecurity risk management, strategy, and governance, Item 106 will reduce information asymmetry and provide investors and other market participants more certainty and easier comparability of registrants' vulnerability to and ability to manage cybersecurity breaches, reducing adverse selection and increasing liquidity. Thus, the final rules could decrease cost of capital across registrants and increase company value, benefiting investors.

One commenter argued that smaller registrants are less likely than larger registrants to experience cybersecurity incidents and that cyberattacks are not material for smaller registrants.[478] This could imply that the degree of cybersecurity-driven adverse selection faced by investors in small registrants might be less severe. If so, the potential benefit from improvement in liquidity and cost of capital due to the timeliness and information benefits from the final rules might be smaller for small registrants and their investors. The research this commenter cited to support this assertion found larger companies were more susceptible than smaller companies to a particular category of cybersecurity incidents—those involving personal information lost through hacking by an outside party—which composed less than one-quarter of

[478] *See* comment letter from BIO. The letter argues that the Commission, when citing the study by Kamiya, et al. (2021) in the Proposing Release, "ignored and omitted" the fact that the mean market capitalization of impacted companies in this study was $58.9 billion, much higher than the average for small companies, and thus "cyberattacks mainly affect large companies and are not material for smaller companies." We observe that an average market capitalization of impacted companies of $58.9 billion would generally indicate that companies both larger and smaller than that size were impacted by cyberattacks.

all cyber incidents in the sample (1,580 out of 6,382).[479] It is possible that malicious strategies that target personal information are particularly suited to larger, well-known companies, and thus the research may overstate the degree to which large companies are more susceptible to cybersecurity incidents generally. These strategies explicitly harm companies' customers, and customer ill will is potentially more newsworthy and consequential for a larger, well-known company as compared to a smaller one. In contrast, ransomware attacks that target non-personal, internal company operations such as an information technology network, for example, are less concerned with causing reputational loss and thus may have an optimal target profile that favors smaller firms as much as larger firms. Additionally, smaller companies may have fewer resources and weaker processes in place to prevent cybersecurity attacks.[480] Hence, it is not clear that smaller companies experience fewer material cybersecurity incidents generally. Others have noted that small companies are frequently targeted victims of cyberattacks, potentially leading to dissolution of the business.[481] Thus, overall, we maintain that cybersecurity attacks are material for smaller reporting companies and that the final rules will serve to benefit them and their investors.

Overall, Form 8-K Item 1.05 and Regulation S-K Item 106 provide for timely, informative, and up-to-date disclosure of cybersecurity incidents, as well as disclosure that may provide insight into whether a registrant is prepared for risks from cybersecurity threats and has adequate cybersecurity risk management, strategy, and governance measures in place to reduce

---

479 *See* Kamiya, et al., *supra* note 413.

480 *See* letter from Tenable.

481 *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 https://docs.house.gov/meetings/SM/SM00/20150422/103276/HHRG-114-SM00-20150422-SD003-U4.pdf* (describing the cybersecurity risks small businesses face and noting "fifty percent of SMB's have been the victims of cyberattack and over 60 percent of those attacked go out of business").

the likelihood of future incidents, reducing the likelihood of delayed or incomplete disclosure and benefiting investors and the market.

We believe enhanced information, timing, and completeness of disclosures as a result of Form 8-K Item 1.05 and Regulation S-K Item 106 will benefit not only investors but also other market participants that rely on registrant disclosures to provide services to investors. They, too, will be able to better evaluate registrants' cybersecurity preparations and risks and thus provide better recommendations. We note that the potential benefit of these amendments could be reduced because some registrants already provide relevant disclosures. That said, we expect this same information will become more useful due to added context from, and easier comparisons with, the increased number of other registrants now providing these 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 final rules. Such 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. One commenter suggested we use existing cyber disclosure models to "empirically determine" the current degree of market mispricing, but did not suggest what data the Commission could use to do so.[482] The Commission cannot estimate the effects of undisclosed cybersecurity incidents that are creating market mispricing, as the relevant information was never released and the market was unable to react.

b. Greater Uniformity and Comparability

The final rules requiring disclosure about cybersecurity incidents and cybersecurity risk management, strategy, and governance should also lead to more uniform and comparable

[482] *See* letter from ISA.

disclosures, in terms of both content and location, benefiting investors by lowering their search and information processing costs. Currently, registrants do not always use Form 8-K to report cybersecurity incidents. Even among registrants that do, reporting practices vary widely.[483] 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. 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, the management's discussion and analysis section, or not at all. For both types of disclosures, the final rules specify the topics that registrants should disclose. As a result, both incident disclosure and risk management, strategy, and governance disclosure should become more uniform across registrants, making them easier for investors and other market participants to compare. The final rules also specify the disclosure locations (e.g., Item 1C of Form 10-K), benefiting investors and other market participants further by reducing the time, cost, and effort it takes them to search for and retrieve information (as pointed out by commenters [484]).

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 believe that Item 106 requires sufficient specificity, tailored to the registrant's facts and circumstances, to help mitigate any tendency towards boilerplate disclosures. Item 106 also provides a non-exclusive list of information that registrants should disclose, as applicable, which should help in this regard.

---

[483] *See* Proposing Release at 16594.

[484] *See, e.g.*, letters from Better Markets; CalPERS.

The requirement to tag the cybersecurity disclosure in Inline XBRL will likely augment the informational and comparability benefits by making the 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.[485] While these observations are specific to operating company financial statement disclosures and not to disclosures outside the financial statements, such as the cybersecurity disclosures, they suggest that the Inline XBRL requirements should 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.[486] Also, unlike XBRL financial statements (including footnotes), which consist of tagged quantitative and narrative disclosures, the cybersecurity disclosures consist largely of tagged narrative disclosures.[487] Tagging narrative disclosures can facilitate analytical benefits

---

485 *See, e.g.*, J.Z. Chen, et al., *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 company 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"). S*ee also* P.A. Griffin, et al., *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 companies by creditors, leading to a reduction in company default risk); 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").

486 *See, e.g.*, N. Trentmann, *Companies Adjust Earnings for Covid-19 Costs, but Are They Still a One-Time Expense?*, WALL ST. 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); R. Hoitash, and U. Hoitash, *Measuring Accounting Reporting Complexity with XBRL*, 93 ACCOUNT. REV. 259 (2018).

487 The cybersecurity disclosure requirements do not expressly require the disclosure of any quantitative values; if a company includes any quantitative values that are nested within the required discussion (e.g., disclosing the

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.[488]

In addition, by formalizing the disclosure requirements related to cybersecurity incidents and cybersecurity risk management, strategy, and governance, the final rules could reduce compliance costs for those registrants that are currently providing disclosure about these topics. The compliance costs would be reduced to the extent that those registrants may be currently over-disclosing information out of caution, to increase the perceived credibility of their disclosures, or to signal to investors that they are diligent with regard to cybersecurity. For instance, the staff has observed that some registrants provide Form 8-K filings even when they do not anticipate the incident will have a material impact on their business operations or financial results.[489] By specifying that only material incidents require disclosure, the final rules should ease some of these concerns and reduce costs to the extent those costs currently exist.[490] Investors will benefit to the extent the registrants they invest in enjoy lower compliance costs.

---

number of days until containment of a cybersecurity incident), those values will be individually detail tagged, in addition to the block text tagging of the narrative disclosures.

488 To illustrate, without Inline XBRL, using the search term "remediation" to search through the text of all companies' filings over a certain period of time, so as to analyze the trends in companies' 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). Inline XBRL, however, enables a user to search for the term "remediation" exclusively within the required cybersecurity disclosures, thereby likely reducing the number of irrelevant results.

489 Based on staff analysis of the 10,941 current and periodic reports in 2022 for companies available in Intelligize and identified as having been affected by a cybersecurity incident using a keyword search.

490 We note that registrants may still over-disclose due to uncertainty over when a cybersecurity incident crosses the threshold of materiality. This may impact how fully costs from immaterial incident disclosure are reduced.

2. Costs

We also recognize that enhanced cybersecurity disclosure would result in costs to registrants, borne by investors. These costs include potential increases in registrants' vulnerability to cybersecurity incidents and compliance costs. We discuss these costs below.

First, the disclosure about cybersecurity incidents and cybersecurity risk management, strategy, and governance could potentially increase the vulnerability of registrants. Since the issuance of the 2011 Staff Guidance, concerns have been raised that providing detailed disclosures of cybersecurity incidents could, potentially, provide a road map for future attacks, and, if the underlying security issues are not completely resolved, could exacerbate the ongoing attack.[491] The concern is that malicious actors could use the disclosures to potentially gain insights into a registrant's practices on cybersecurity. As a result, the final incident disclosure rules could potentially impose costs on registrants and their investors, if, for example, additional threat actors steal more data or hamper breach resolution.

The final rules have been modified from the Proposing Release to mitigate disclosure of details that could aid threat actors, while remaining informative for investors. Form 8-K Item 1.05 will require registrants to timely disclose material cybersecurity incidents, describe the material aspects of the nature, scope, and timing of the incident, and, importantly, describe the material impact or reasonably likely material impact of the incident on the registrant. Focusing on the material impact or reasonably likely material impact of the incident rather than the specific or technical details of the incident should reduce the likelihood of providing a road map

[491] *See*, *e.g.*, Roland L. Trope & 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).

that threat actors can exploit for future attacks, and should reduce the risks and costs stemming from threat actors acting in this manner.[492]

Similar concerns were raised by commenters about the required risk management, strategy, and governance disclosure.[493] Items 106(b) and (c) require registrants to provide specified disclosure regarding their cybersecurity risk management processes and cybersecurity governance by the management and board. The required disclosure could provide malicious actors information about which registrants have weak processes 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 necessarily lead to more attacks. 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.[494] Another study finds that cybersecurity risk factor disclosures that involve terms about processes are less likely to be related to future breach announcements than disclosures that employ more general language.[495] On the other hand, we note that the final rules will require more details of cybersecurity processes than what is explicitly required under the current rules, and the uniformity of the final rules might also make it easier for malicious actors to identify registrants with relatively weaker

---

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

493 *See* letters from ABA; ACLI; APCIA; BIO; BPI et al.; Business Roundtable; Chamber; CSA; CTIA; EIC; Enbridge; FAH; Federated Hermes; GPA; ITI; ISA; Nareit; NAM; NMHC; NRA; NRF; SIFMA; Sen. Portman; TechNet; TransUnion; USTelecom; Virtu; *see also supra* note 201 and accompanying text.

494 *See* He Li, Won Gyun No, & Tawei Wang, *SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors*, 30 INT'L. J. OF ACCT. INFO. SYS. 40-55 (2018) ("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").

495 *See* Tawei Wang, Karthik N. Kannan, & Jackie Rees Ulmer, *The Association Between the Disclosure and the Realization of Information Security Risk Factors*, 24.2 INFO. SYS. RES. 201, 201-218 (2013).

processes. Therefore, these academic findings might not be generalizable to the effects of the final rules.[496] However, we also note that we have streamlined the disclosure obligations for Items 106 (b) and (c), in response to commenters' concerns, to require a more principles-based discussion of a registrant's processes instead of detailed disclosures on a specific set of items. This change should help ease concerns that the required cybersecurity risk management, strategy, and governance disclosures will help malicious actors choose targets. In addition, the potential costs resulting from the disclosure requirements might be partially mitigated to the extent that registrants decide to enhance their cybersecurity risk management in anticipation of the increased disclosure. This possibility is discussed below under Indirect Economic Effects.

The final rules will also impose compliance costs. Registrants, and thus their investors, will incur one-time and ongoing costs to fulfill the new disclosure requirements under Item 106 of Regulation S-K. These costs will include costs to gather the information and prepare the disclosures. Registrants will also incur compliance costs to fulfill the disclosure requirements related to Form 8-K (Form 6-K for FPIs) incident disclosure.[497] 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 will disclose such incident with the required information within four business days. Registrants may also incur ongoing costs to disclose in a Form 8-K report any material changes or updates relating to previously disclosed incidents, and we expect these costs to be higher for registrants with more incidents to disclose. The costs will be mitigated for registrants whose current disclosure practices match or are similar

[496] We note that the papers we cited above study the effect of voluntary disclosure and the 2011 Staff Guidance, which could also reduce the generalizability of these studies to the mandatory disclosures under the final rules.

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

to those that are in the final rules. One commenter suggested that companies could incur costs to reconcile their existing cybersecurity activities and NIST-based best practices with the requirements of the final rules[498] but, as discussed in Section II.C.3.c, the final rules are not in conflict with NIST and we do not anticipate that significant reconciliation will be needed.

The compliance costs will also include costs attributable to the Inline XBRL tagging requirements. Many commenters supported the XBRL tagging requirement,[499] while one commenter suggested that it would be burdensome to add tagging given the time-sensitive nature of the disclosure requirements.[500] 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.[501] The incremental compliance costs associated with Inline XBRL tagging of cybersecurity disclosures will also be mitigated by the fact that most companies that will be subject to the 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

---

498 *See* letter from SIFMA.

499 *See* letters from E&Y; CAQ; PWC; NACD; AICPA; XBRL.

500 *See* letter from NYC Bar.

501 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* AICPA, *XBRL Costs for Small Companies Have Declined 45% since 2014* (2018), *available at https://us.aicpa.org/content/dam/aicpa/interestareas/frc/accountingfinancialreporting/xbrl/downloadabledocuments/xbrl-costs-for-small-companies.pdf*. *See also* Letter from Nasdaq, Inc. (Mar. 21, 2019) (responding to *Request for Comment on Earnings Releases and Quarterly Reports*, Release No. 33-10588 (Dec. 18, 2018) [83 FR 65601 (Dec. 21, 2018)]) (stating that a 2018 NASDAQ survey of 151 listed companies 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).

statements.[502] Such companies may be able to leverage existing Inline XBRL preparation processes and expertise in complying with the cybersecurity disclosure tagging requirements. Moreover, the one-year XBRL compliance period extension could further assuage concerns about the transition for registrants to comply with the new requirements.[503]

Some commenters contended that the Proposing Release failed to consider the costs of the proposed rules adequately.[504] We are generally unable to quantify costs related to the final rules due to a lack of data. For example, we are unable to quantify the impact of any increased vulnerability to existing or new threat actors arising from the required incident or risk management, strategy, or governance disclosures. Moreover, costs related to preparing cyber-related disclosures are generally private information known only to the issuing firm, hence such data are not readily available to the Commission. There is also likely considerable variation in these costs depending on a given firm's size, industry, complexity of operations, and other characteristics, which makes comprehensive estimates difficult to obtain. We note that the Commission has provided certain estimates for purposes of compliance with the Paperwork Reduction Act of 1995, as further discussed in Section V below. Those estimates, while useful to understanding the collection of information burden associated with the final rules, do not purport to reflect the full costs associated with making the required disclosures.

One commenter provided a numerical cost estimate, stating the initial costs of complying with the proposed rules would be $317.5 million to $523.4 million ($38,690 to $69,151 per regulated company), and future annual costs would be $184.8 million to $308.1 million ($22,300

---

[502] *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).

[503] *See supra* Section II.I.

[504] *See, e.g.,* letters from Chamber and SIFMA.

to $37,500 per regulated company).[505] We cannot directly evaluate the accuracy of these estimates because the commenter did not provide any explanation for how they were derived. We believe, however, these estimates likely significantly overstate the costs of the final rules.

First, the commenter overestimates the number of registrants who are likely to bear the full costs of new disclosures. Converting the total and per company cost estimates to registrant counts implies the commenter assumed these costs would be borne by approximately 8,000 companies, which would be nearly every registrant.[506] As stated in Section IV.B.2 above, however, 73 percent of domestic filers in 2022 already made cybersecurity-related disclosures in Form 10-K filings and amendments, and 35 Form 8-K filings disclosed material cybersecurity incidents.[507] While the degree to which registrants' existing disclosures already may be in line with the requirements of the final rules varies—some registrants may need to make significant changes while others may not, especially given the guidance from the 2018 Interpretive Release—most registrants should not bear the full costs of compliance. In addition, while cybersecurity incident disclosure is expected to increase as a result of Item 1.05, we do not expect that most companies will need to report in any given year. Extrapolating from the current numbers of incidents reported—for example, public companies disclosed 188 reported breaches in 2021[508]—we expect that the overwhelming majority of registrants will not experience a material breach and will not need to disclose cybersecurity incidents and incur the ongoing

---

505 *See* letter from Chamber.

506 $317.5 million divided by $38,690 per registrant equals 8,206 registrants; $523.4 million divided by $69,151 per registrant equals 7,569 registrants; $184.8 million divided by $22,300 per registrant equals 8,287 registrants; $308.1 million divided by $37,500 per registrant equals 8,216 registrants. In Section IV.B.2, *supra*, we find the number of affected parties to include approximately 7,300 operating companies filing on domestic forms and 1,174 FPIs filing on foreign forms.

507 *See supra* notes 456 and 457 and accompanying text.

508 *See supra* note 426 and accompanying text.

associated costs.[509] They may, however, revisit their disclosure controls initially, to ensure they are capturing what the rule requires.

Second, we have made changes from the proposed rules that would also reduce costs as compared with the proposal. Some of these changes concerned aspects of the proposed rules that the commenter noted would be burdensome. For example, the commenter states that "potential material incidents in the aggregate would be difficult to identify and operationally challenging to track."[510] The commenter also states "the SEC underestimates the burdens related to tracking 'several small but continuous cyberattacks against a company,' which may or may not prove to be material."[511] These comments refer to proposed Item 106(d)(2), which would have required disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. In response to comments, we are not adopting this aspect of the proposal and instead have added "a series of related unauthorized occurrences" to the definition of "cybersecurity incident," which may help address this concern about the burden of the proposal. The comment letter also stated that "cybersecurity talent is scar[c]e globally. From a personnel standpoint, it's unclear where companies would get the so-called cybersecurity experts that the proposed regulation would mandate. There is a well-documented lack of cybersecurity talent for the public and private sectors that would unquestionably affect companies' recruitment of board cybersecurity experts."[512] We are not adopting proposed 407(j) about the cybersecurity expertise, if any, of a registrant's board members, which may have factored into the commenter's cost estimates. Additionally, the proposal would not have

---

509 This conclusion is based on relative quantities. Note that 188 is very small relative to the total number of registrants, 8,474, from Section IV.B.2 (188 divided by 8,474 is roughly 2%).

510 *See* letter from Chamber.

511 *Id*.

512 *Id*.

mandated recruitment of cybersecurity experts, only disclosure of their presence. Additional streamlining of requirements in the final rules (e.g., reduced granularity of cybersecurity incident disclosure requirements) should further reduce costs from what might have been estimated using the Proposing Release.

Another commenter stated that the Commission's calculation of costs and benefits does not adequately address the impact of different but overlapping disclosure and reporting requirements that may escalate burdens and costs.[513] We acknowledge the possibility that to the extent different information has to be reported pursuant to different regulations, laws, or other requirements, there could be a greater cost because of the demands to keep track of and manage the multiple different disclosure regimes. However, to the extent that certain other existing requirements may involve monitoring cybersecurity incidents or assessing an incident's impact on the registrant, the registrant may be able to leverage existing disclosures to reduce the burden of complying with the final rules. Additionally, as noted in Section II.A.3 those other regulations generally serve different purposes than the final rules, and we believe that the benefits of the final rules justify the costs.

One commenter raised a concern that the costs of the rules reached the threshold of an "economically significant rulemaking" under the Unfunded Mandate Reform Act of 1995 ("UMRA") and the Small Business Regulatory Enforcement Fairness Act, thus requiring an "enhanced economic analysis."[514] The requirement to issue an analysis under the UMRA does not apply to rules issued by independent regulatory agencies.[515]

---

513 See letter from SIFMA.

514 *See* letter from Chamber.

515 *See* 2 U.S.C. 658 ("The term 'agency' has the same meaning as defined in section 551(1) of title 5, United States Code, but does not include independent regulatory agencies."). *See also* Congressional Research Service,

The compliance costs of the final rules could be disproportionately burdensome to smaller registrants, as some of these costs may have a fixed component that does not scale with the size of the registrant.[516] Also, smaller registrants may have fewer resources with which to implement these changes.[517] One commenter suggested this could lead some small companies seeking to conduct an initial public offering to reconsider.[518] Commenters also noted that smaller companies may not yet have a mature reporting regime and organizational structure and would benefit from an onramp to compliance.[519] We are not adopting some proposed requirements (e.g., disclosing whether the board includes a cybersecurity expert), and thus the cost burden of the final rules should not be as high as initially proposed. We also are delaying compliance for incident disclosure for smaller reporting companies by providing an additional phase-in period of 180 days after the non-smaller reporting company compliance date for smaller reporting companies, which will delay compliance with these requirements for 270 days from effectiveness of the rules.[520] To the extent smaller reporting companies are less likely than larger companies to have incident disclosure processes in place, they could benefit from additional time to comply. An extended compliance date may also permit smaller reporting companies to benefit from seeing how larger companies implement these disclosures. Investors in these smaller registrants could benefit from higher disclosure quality afforded by the delay, although

Unfunded Mandates Reform Act: History, Impact, and Issues (July 17, 2020), *available at https://sgp.fas.org/crs/misc/R40957.pdf* (noting "[UMRA] does not apply to duties stemming from participation in voluntary federal programs [or] rules issued by independent regulatory agencies").

516 *See infra* Section VI.

517 *See, e.g.*, letter from SBA.

518 *See* letter from BIO.

519 *See, e.g.*, letter from BIO.

520 *See supra* Section II.I.

some benefits, such as the reduction in asymmetric information and mispricing, would also be delayed.

3. Indirect Economic Effects

While the final rules only require disclosures—not changes to risk management practices—the requirement to disclose and the disclosures themselves could result in certain indirect benefits and costs. In anticipating investor reactions to the required disclosures, for example, registrants might devote more resources to cybersecurity governance and risk management in order to be able to disclose those efforts. Although not the purpose of this rule, registrants devoting resources to cybersecurity governance and risk management could reduce both their susceptibility to a cybersecurity attack, reducing the likelihood of future incidents, as well as the degree of harm suffered from an incident, benefiting registrants and investors. The choice to dedicate these resources would also represent an indirect cost of the final rules, to the extent registrants do not already have governance and risk management measures in place. As with compliance costs, the cost of improving cybersecurity governance and risk management could be proportionally higher for smaller companies if these registrants have fewer resources to implement these changes, and to the extent these costs do not scale with registrant size.

In addition, the 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 have been observed to reduce information processing cost. This reduction in information processing cost has been observed to facilitate the monitoring of registrants by other market participants, and, as a result, to influence registrants' behavior, including their disclosure choices.[521]

[521] *See supra* note 485.

The requirement in Item 1.05 that registrants timely disclose material cybersecurity incidents could also indirectly affect consumers, and external stakeholders such as other registrants in the same industry and those facing similar cybersecurity threats. Cybersecurity incidents can harm not only the company that suffers the incident but also other businesses and consumers. For example, a cybersecurity breach at one company, such as a gas pipeline, or a power company, may cause a major disruption or shutdown of a critical infrastructure industry, resulting in broad losses throughout the economy.[522] Timely disclosure of cybersecurity incidents required by Item 1.05 could increase awareness by those external stakeholders and companies in the same industry that the malicious activities are occurring, giving them more time to mitigate any potential damage.

To the extent that Item 1.05 increases incident disclosure, consumers may learn about a particular cybersecurity breach and therefore take appropriate actions to limit potential economic harm that they may incur from the breach. For example, there is evidence that increased disclosure of cybersecurity incidents by companies can reduce the risk of identity theft for individuals.[523] Also, consumers may be able to make better informed decisions about which companies to entrust with their personal information.

---

[522] See Lawrence A. Gordon, et al., *Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model*, 6 J. INFO. SEC. 24, 25 (2015) ("Firms 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."). *See also* Collin Eaton and Dustin Volz, *U.S. Pipeline Cyberattack Forces Closure*, WALL ST. J. (MAY 8, 2021), *available at https://www.wsj.com/articles/cyberattack-forces-closure-of-largest-u-s-refined-fuel-pipeline-11620479737*.

[523] *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%).

As discussed above, to the extent that registrants may decide to enhance their cybersecurity risk management in anticipation of the increased disclosure, that could reduce registrants' susceptibility to and damage incurred from a cybersecurity attack. This reduced likelihood of and vulnerability to future incidents could reduce the negative externalities of those incidents, leading to positive spillover effects and a reduction in overall costs to society from these attacks.

However, the magnitude of this and the other indirect effects discussed above would depend upon factors outside of the specific disclosures provided in response to the final rule, and therefore it is difficult to assess with certainty the likelihood or extent of these effects.

D. Effects on Efficiency, Competition, and Capital Formation

We believe the final rules should have positive effects on market efficiency. As discussed above, the final rules should improve the timeliness and informativeness of cybersecurity incident and risk disclosure. As a result of the disclosure required by the final rules, investors and other market participants should better understand the cybersecurity threats registrants are facing, their potential impact, and registrants' ability to respond to and manage risks. Investors and other market participants should thereby better evaluate registrants' securities and make more informed decisions. As a result, the required disclosures should reduce information asymmetry and mispricing in the market, improving market efficiency. More efficient prices should improve capital formation by increasing overall public trust in markets, leading to greater investor participation and market liquidity.

The final rules also could promote competition among registrants with respect to improvement in both their cybersecurity risk management and transparency in communicating their cybersecurity processes. To the extent investors view strong cybersecurity risk

management, strategy, and governance favorably, registrants disclosing more robust processes, more clearly, could benefit from greater interest from investors, leading to higher market liquidity relative to companies that do not. Customers may also be more likely to entrust their business to companies that protect their data. Registrants that to date have invested less in cybersecurity preparation could thus be incentivized to invest more, to the benefit of investors and customers, in order to become more competitive. To the extent that increased compliance costs resulting from the final rules prevent smaller companies from entering the market, as a commenter suggested,[524] the final rules could reduce the ability of smaller companies to compete and thereby reduce competition overall.

E. Reasonable Alternatives

1. Website Disclosure

As an alternative to Form 8-K disclosure of material cybersecurity incidents, we considered providing registrants with the option of disclosing this information instead through company websites, if the company 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 company because it may involve fewer compliance costs, disclosures made on company websites would not be located in a central depository, such as the EDGAR system,[525] and would not be in the same place as other registrants' disclosures of material cybersecurity incidents, nor would they be organized into the standardized sections found in Form 8-K and could thus be less uniform. Even if we required registrants to announce the

---

[524] *See* letter from BIO.

[525] 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.

disclosure, or to alert the Commission to it, the information would still be more difficult for investors and market participants to locate and less uniform than Form 8-K.

The lack of a central repository, 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 on the EDGAR system when the disclosure is filed with the Commission, because registrants may not keep historical information available on their websites indefinitely and it could be difficult to determine whether the website information had moved or changed. Therefore, this approach would be less beneficial to investors, other market participants, and the overall efficiency of the market.

2. Disclosure through Periodic Reports

We also considered requiring disclosure of material cybersecurity incidents through quarterly or annual reports, as proposed, 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 to file as frequently. And, it might further reduce the risk that disclosure could provide timely information to attackers.

However, this alternative also 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 securities 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 requirements of Item 1.05. Additionally, as previously discussed, less timely reporting could adversely impact external stakeholders, such as other registrants in the same industry and those facing similar cybersecurity threats, and consumers whose data were compromised.

Relatedly, we proposed requiring registrants to disclose material changes and additions to previously reported cybersecurity incidents on Forms 10-K and 10-Q instead of on an amended Form 8-K. However, as discussed above, we believe using Form 8-K would be more timely and consistent;[526] all disclosures concerning material cybersecurity incidents, whether new or containing information not determined or unavailable initially, will be disclosed on the same form.

3. Exempt Smaller Reporting Companies

We also considered exempting smaller reporting companies from the final rules.[527] Exempting smaller reporting companies from the disclosure requirements of the final rules would avoid compliance costs for smaller companies, including those compliance costs that could disproportionately affect smaller companies.[528] As noted earlier, however, we are not adopting some proposed requirements (e.g., disclosing whether the board includes a cybersecurity expert) and modifying others (e.g., requiring a description of cybersecurity "processes" instead of more formal "policies and procedures"), and thus the cost burden of the final rules should not be as high as initially proposed. This should mitigate some of the concerns raised by commenters and would also reduce the potential value of an exemption. Moreover, an exemption would remove the benefit to investors of informative, timely, uniform, and

[526] *See supra* Section II.B.3.

[527] *See supra* Section II.G.2.

[528] *See supra* Section II.G.2

comparable disclosure with regard to smaller companies. And although one commenter argued for an exemption based on a perception that smaller companies are less likely to experience cybersecurity incidents,[529] for the reasons explained in Section IV.C.1.b, we believe that smaller companies are still at risk for material cybersecurity incidents. This aligns with comments we received opposing an exemption for smaller reporting companies.[530]

Lastly, one commenter that argued for an exemption cited the Proposing Release, which noted a potential for increased cost of capital for registrants that do not have cybersecurity programs once disclosures are mandated; the commenter stated that these would disproportionately be smaller registrants.[531] We have reconsidered the argument that registrants without robust cybersecurity processes in place might face a higher cost of capital and as a result would be priced unfavorably, and no longer believe it to be accurate. It is indeed possible that companies that reveal what investors consider to be less robust cybersecurity risk management, strategy, and governance processes may experience a decline in stock price. However, because the risk of cybersecurity attacks should be idiosyncratic, this decline would likely be due to investors updating their expectations of future cash flows for this firm to incorporate higher likelihood of a future incident—moderating the decline should future incidents occur—not an increase in fundamental market risk and thus cost of capital. In addition, to the extent investors already rationally anticipate that smaller registrants or registrants that have not previously disclosed such information have less robust policies, there may be less or no stock price decline as a result of Item 106, as these disclosures would merely confirm expectations. Thus, increases

529 *See* letter from BIO.

530 *See*, *e.g.*, letters from Cybersecurity Coalition; Tenable.

531 *See* letter from BIO.

in cost of capital should not be prevalent in this regard and should not be a reason to exempt small firms from the final rules.

V. PAPERWORK REDUCTION ACT

A. Summary of the Collections of Information

Certain provisions of our rules and forms that will be affected by the final rules contain "collection of information" requirements within the meaning of the Paperwork Reduction Act ("PRA").[532] The Commission published a notice requesting comment on changes to these collections of information in the Proposing Release and submitted these requirements to the Office of Management and Budget ("OMB") for review in accordance with the PRA.[533]

The hours and costs associated with preparing, filing, and sending 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:[534]

- "Form 8-K" (OMB Control No. 3235-0060);
- "Form 6-K" (OMB Control No. 3235-0116);
- "Form 10-K" (OMB Control No. 3235-0063); and
- "Form 20-F" (OMB Control No. 3235-0288).

---

[532] 44 U.S.C. 3501 *et seq*.

[533] 44 U.S.C. 3507(d) and 5 CFR 1320.11.

[534] The Proposing Release also listed "Schedule 14A" (OMB Control No. 3235-0059), "Schedule 14C" (OMB Control No. 3235-0057), and "Form 10-Q" (OMB Control No. 3235-0070) as affected collections of information. However, under the final rules, these schedules and form are no longer affected.

The Commission adopted all of the existing regulations and forms pursuant to the Securities Act and the Exchange Act. The regulations and forms set forth disclosure requirements for current reports and periodic reports filed by registrants to help shareholders make informed voting and investment decisions.

A description of the final amendments, including the need for the information and its 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 final amendments can be found in Section IV above.

B. Summary of Comment Letters and Revisions to PRA Estimates

In the Proposing Release, the Commission requested comment on the PRA burden hour and cost estimates and the analysis used to derive the estimates.[535] While a number of parties commented on the potential costs of the proposed rules, only one commenter spoke specifically to the PRA analysis, arguing that the proposal "cannot be justified under the Paperwork Reduction Act" because of an "unreasonable" number of separate disclosures and because "the amount of information the Proposal would require to be produced is unwarranted in light of other, existing regulations."[536] The commenter further alleged that the Proposing Release's "calculation of costs and benefits is skewed" because "[d]ifferent but overlapping disclosure and reporting requirements do not correlate with lower burdens on information providers, but rather, escalated burdens and costs."

While we acknowledge the commenter's concerns about costs of the proposal, for the reasons discussed in Section II.H and elsewhere throughout this release, we believe the information required by the final rules is necessary and appropriate in the public interest and for

[535] Proposing Release at 16616-16617.

[536] *See* letter from SIFMA.

the protection of investors. Further, a discussion of the economic effects of the final amendments, including consideration of comments that expressed concern about the expected costs associated with the proposed rules, can be found in Section IV above. With regard to the calculation of paperwork burdens, we note that both the Proposing Release's PRA analysis and our PRA analysis of the final amendments here estimate the incremental burden of each new or revised disclosure requirement individually and fully comport with the requirements of the PRA. Our estimates reflect the modifications to the proposed rules that we are adopting in response to commenter concerns, including streamlining some of the proposed rule's elements to address concerns regarding the level of detail required and the anticipated costs of compliance.

C. Effects of the Amendments on the Collections of Information

The following PRA Table 1 summarizes the estimated effects of the final amendments on the paperwork burdens associated with the affected collections of information listed in Section V.A.

PRA Table 1 – Estimated Paperwork Burden of Final Amendments

Final Amendments and Effects	Affected Forms	Estimated Burden Increase	Number of Estimated Affected Responses*
Form 8-K • Add Item 1.05 requiring disclosure of material cybersecurity incidents within four business days following determination of materiality.	Form 8-K	9 hour increase in compliance burden per form	200 Filings
Form 6-K • Add "cybersecurity incident" to the list in General Instruction B of information required to be furnished on Form 6-K.	Form 6-K	9 hour increase in compliance burden per form	20 Filings
Regulation S-K Item 106 • Add Item 106(b) requiring disclosure regarding cybersecurity risk management and strategy. • Add Item 106(c) requiring disclosure regarding cybersecurity governance.	Form 10-K and Form 20-F	Form 10-K: 10 hour increase in compliance burden per form Form 20-F: 10 hour increase in compliance burden per form	8,292 Filings 729 Filings

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

The estimated burden increases for Forms 8-K, 10-K, and 20-F reflect changes from the estimates provided in the Proposing Release. There, the Commission estimated that the average incremental burden for an issuer to prepare the Form 8-K Item 1.05 disclosure would be 10 hours. The proposed estimate included the time and cost of preparing the disclosure, as well as tagging the data in XBRL. The changes we are making to Item 1.05 in the final rules should generally reduce the associated burden by an incremental amount in most cases. We therefore estimate that Form 8-K Item 1.05 will have a burden of 9 hours, on par with the average burdens of existing Form 8-K items, which is 9.21 hours.

In the Proposing Release, the Commission estimated that the average incremental burden for preparing Form 10-K stemming from proposed Item 106 would be 15 hours. Similarly, the Commission estimated that proposed Item 106 would result in an average incremental burden for preparing Form 20-F of 16.5 hours. The proposed estimates included the time and cost of preparing the disclosure, as well as tagging the data in XBRL. We estimate the changes we are

making to Item 106 in the final rules should generally reduce the associated burden by one-third due to the elimination of many of the proposed disclosure items; accordingly, we have reduced the estimated burden to 10 hours from 15 hours for Form 10-K, and to 10 hours from 16.5 hours for Form 20-F.[537]

We have not modified the estimated number of estimated affected responses for Form 8-K and Form 6-K from what was proposed. As noted in the Proposing Release, not every filing of these forms would include responsive disclosures. Rather, 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.

D. Incremental and Aggregate Burden and Cost Estimates for the Final Amendments

Below we estimate the incremental and aggregate increase in paperwork burden as a result of the final 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 and from year to year based on a number of factors, including the nature of their business.

The burden estimates were calculated by multiplying the estimated number of responses by the estimated average amount of time it would take a registrant to prepare and review disclosure required under the final amendments. For purposes of the PRA, the burden is to be

[537] Note that, in the proposal, a portion of the burden for companies reporting on Form 10-K was allocated to Schedule 14A, as a result of certain disclosure items being proposed to be included in Rule 407 of Regulation S-K. By contrast, since registrants reporting on Form 20-F do not have an analogous form to Schedule 14A, the comparable burden to Schedule 14A was attributable to Form 20-F. Since we are not adopting Item 407 as proposed, and we do not expect any disclosures on Schedule 14A, the estimates for Form 10-K and Form 20-F are now aligned.

allocated between internal burden hours and outside professional costs. PRA Table 2 below sets forth the percentage estimates we typically use for the burden allocation for each collection of information. We also estimate that the average cost of retaining outside professionals is $600 per hour.[538]

PRA Table 2: Standard Estimated Burden Allocation for Specified Collections of Information

Collection of Information	Internal	Outside Professionals
Form 10-K, Form 6-K, and Form 8-K	75%	25%
Form 20-F	25%	75%

PRA Table 3 below illustrates the incremental change to the total annual compliance burden of affected collections of information, in hours and in costs, as a result of the final amendments.

[538] 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 $600 per hour. At the proposing stage, we used an estimated cost of $400 per hour. We are increasing this cost estimate to $600 per hour to adjust the estimate for inflation from Aug. 2006.

PRA Table 3. Calculation of the Incremental Change in Burden Estimates of Current Responses Resulting from the Final Amendments

Collection of Information	Number of Estimated Affected Responses (A)*	Burden Hour Increase per Response (B)	Change in Burden Hours (C) = (A) x (B)**	Change in Company Hours (D) = (C) x 0.75 or .25	Change in Professional Hours (E) = (C) x 0.25 or .75	Change in Professional Costs (F) = (E) x $600
8-K	200	9	1,800	1,350	450	$270,000
6-K	20	9	180	135	45	$27,000
10-K	8,292	10	82,920	62,190	20,730	$12,438,000
20-F	729	10	7,290	1,822.50	5,467.50	$3,280,500

* The number of estimated affected responses is based on the number of responses in the Commission's current OMB PRA filing inventory. The OMB PRA filing inventory represents a three-year average.

** The estimated changes in Columns (C), (D), and (E) are rounded to the nearest whole number.

The following PRA Table 4 summarizes the requested paperwork burden, including the estimated total reporting burdens and costs, under the final amendments.

PRA Table 4. Requested Paperwork Burden Under the Final Amendments

	Current Burden			Program Change			Revised Burden		
Form	Current Annual Responses (A)	Current Burden Hours (B)	Current Cost Burden (C)	Change in Number of Affected Responses (D)	Change in Company Hours (E)†	Change in Professional Costs (F)‡	Annual Responses (G) = (A)+(D)	Burden Hours (H) = (B) + (E)	Cost Burden (I) = (C) + (F)
Form 8-K	118,387	818,158	$108,674,430	200	1,350	$270,000	118,587	819,508	$108,944,430
Form 6-K	34,794	227,031	$30,270,780	20	135	$27,000	34,814	227,166	$30,297,780
Form 10-K	8,292	13,988,770	$1,835,588,919	--	62,190	$12,438,000	8,292	14,050,960	$1,848,026,919
Form 20-F	729	478,983	$576,490,625	--	1,822.50	$3,280,500	729	480,805.50	$579,771,125

† From Column (D) in PRA Table 3

‡ From Column (F) in PRA Table 3

VI. FINAL REGULATORY FLEXIBILITY ANALYSIS

The Regulatory Flexibility Act ("RFA") requires the Commission, in promulgating rules under Section 553 of the Administrative Procedure Act,[539] to consider the impact of those rules on small entities. We have prepared this Final Regulatory Flexibility Analysis ("FRFA") in accordance with Section 604 of the RFA.[540] An Initial Regulatory Flexibility Analysis ("IRFA") was prepared in accordance with the RFA and was included in the Proposing Release.[541]

A. Need for, and Objectives of, the Final Amendments

The purpose of the final amendments is to ensure investors and other market participants receive timely, decision-useful information about registrants' material cybersecurity incidents, and periodic information on registrants' approaches to cybersecurity risk management, strategy, and governance that is standardized and comparable across registrants. The need for, and objectives of, the final rules are described in Sections I and II above. We discuss the economic impact and potential alternatives to the amendments in Section IV, and the estimated compliance costs and burdens of the amendments under the PRA in Section V.

B. Significant Issues Raised by Public Comments

In the Proposing Release, the Commission requested comment on any aspect of the IRFA, and particularly on the number of small entities that would 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.

---

539 5 U.S.C. 553.

540 5 U.S.C. 604.

541 Proposing Release at 16617.

We received one comment letter on the IRFA, from the U.S. Small Business Administration's Office of Advocacy ("Advocacy").[542] Advocacy's letter expressed concern that "the IRFA does not adequately describe the regulated small entities and potential impacts on those entities."[543] In the Proposing Release, the Commission estimated that the proposed amendments would apply to 660 issuers and 9 business development companies that may be considered small entities.[544] Advocacy's comment letter stated that this estimate did "not provide additional information, such as the North American Industry Classification System ("NAICS") classifications of the affected entities" and did not "break down the affected entities into smaller size groups (e.g., based on total assets)."[545] It also stated that the IRFA did not "adequately analyze the relative impact of costs to small entities."[546] In this vein, it suggested that emerging growth companies ("EGCs") may face particular challenges complying with the proposed rules.[547] In particular, Advocacy's comment letter stated that "[e]merging growth companies may have little or no revenue to afford the additional cost burden of the proposed rules and may not have access to the cybersecurity expertise necessary to comply with the new disclosure requirements."[548]

---

542 *See* letter from U.S. Small Business Administration Office of Advocacy. We also received some comments that, while not specifically addressed to the IRFA, did concern the impact of the proposed rules on smaller reporting companies. *See* letters from BDO; BIO; CSA; Cybersecurity Coalition; NACD; NASAA; Nasdaq; NDIA; Prof. Perullo; Tenable. We have addressed those comments in Section II.G.2, *supra*, and incorporate those responses here as applicable to our RFA analysis. We also note the recommendations for all Commission rulemakings from the Office of the Advocate for Small Business Capital Formation. *See* 2022 OASB Annual Report.

543 *Id.*

544 Proposing Release at 16617.

545 *See* letter from Advocacy.

546 *Id.*

547 *Id.*

548 *Id.*

The comment letter from Advocacy also addressed the discussion of alternatives within the IRFA and the Commission's explanation of why it did not ultimately propose such alternatives. Advocacy stated that "[t]he RFA requires that an IRFA provide significant, feasible alternatives that accomplish an agency's objectives," and stated that the IRFA did not satisfy this requirement because it listed "broad categories of potential alternatives to the proposed rules but [did] not analyze any specific alternative that was considered by the SEC," and because it did not "contain a description of significant alternatives which accomplish the stated SEC objectives and which minimize the significant economic impact of the proposal on small entities."

1. Estimate of Affected Small Entities and Impact to Those Entities

With respect to the adequacy of the Proposing Release's estimate of affected small entities, the RFA requires "a description of and, where feasible, an estimate of the number of small entities to which the proposed rule will apply."[549] Advocacy's published guidance recommends agencies use NAICS classifications to help in "identifying the industry, governmental and nonprofit sectors they intend to regulate."[550] Here, given that the rulemaking applies to and impacts all public company registrants, regardless of industry or sector, we do not believe that further breakout of such registrants by industry classification is necessary or would otherwise be helpful to such entities understanding the impact of the proposed or final rules. This is not a case in which small entities in certain industries and sectors would be affected more than others, as cybersecurity risks exist across industries.[551] For the same reasons we are not

---

549 5 U.S.C. 603(b)(3).

550 U.S. Small Business Administration Office of Advocacy, *A Guide for Government Agencies: How to Comply with the Regulatory Flexibility Act* (Aug. 2017), at 18, *available at https://www.sba.gov/sites/default/files/advocacy/How-to-Comply-with-the-RFA-WEB.pdf*.

551 A breakout would be relevant where, for example, the Commission finds that small entities generally would not be affected by a rule but small entities in a particular industry would be affected.

breaking down the affected entities into smaller size groups (e.g., based on total assets) as recommended by Advocacy. Given the nature of the final rules, we believe that our estimate of the number of small entities to which the final rules will apply adequately describes and estimates the small entities that will be affected.[552]

With respect to Advocacy's suggestion that the proposed rule may be "particularly problematic" for EGCs, we have discussed in Section IV.C.2 above the anticipated costs of the final rules, including their impact on EGCs. We also note that the category of EGC is not the same as the category of "small entity" for purposes of the RFA, and indeed EGC status is not a reliable indicator of whether a registrant is a small entity.[553] While EGC status does include a revenue component, it importantly considers whether the issuer is *seasoned*, meaning, whether it is a new registrant (rather than a registrant with a longer public reporting history). Accordingly, while many EGCs are small entities, there are many that are not. Likewise, many small entities are not EGCs. For purposes of the FRFA, our focus is on the impact on small entities, regardless of whether or not they are EGCs.

We disagree with the statement in the Advocacy comment letter that "SEC expects that the costs associated with the proposed amendments to be similar for large and small entities." The Commission explained in the IRFA that the proposed amendments would apply to small entities to the same extent as other entities, irrespective of size, and that therefore, the Commission expected that "the *nature* of any benefits and costs associated with the proposed

---

552 *See infra* Section VI.C.

553 An EGC is defined as a company that has total annual gross revenues of less than $1.235 billion during its most recently completed fiscal year and, as of Dec. 8, 2011, had not sold common equity securities under a registration statement. A company continues to be an EGC for the first five fiscal years after it completes an initial public offering, unless one of the following occurs: its total annual gross revenues are $1.235 billion or more; it has issued more than $1 billion in non-convertible debt in the past three years; or it becomes a "large accelerated filer," as defined in Exchange Act Rule 12b-2.

amendments to be similar for large and small entities" (emphasis added).[554] The analysis with respect to the *nature* of the costs (and benefits) of the proposed rules detailed in the Economic Analysis of the Proposing Release was referenced in the IRFA to help small entities understand such impacts, not to imply that small entities face the same degree of costs as large entities. Indeed, the Commission went on to state in both the IRFA and the Economic Analysis of the Proposing Release that, while it was unable to project the economic impacts on small entities with precision, it recognized that "the costs of the proposed amendments borne by the affected entities could have a proportionally greater effect on small entities, as they may be less able to bear such costs relative to larger entities."[555] Additionally, in Section IV, above, we discuss the economic effects, including costs, of the final amendments across all entities. We recognize that to the extent the costs are generally uniform across all entities, they would have a relatively greater burden on smaller entities. That said, as discussed both above and below, to help mitigate that relatively greater burden and to respond to comment letters including the letter from Advocacy, we have extended the compliance date for smaller reporting companies so as to provide additional transition time and allow them to benefit from the experience of larger companies. Accordingly, we believe that both this FRFA and our prior IRFA adequately describe and analyze the relative impact of costs to small entities.

2. Consideration of Alternatives

The IRFA's discussion of significant alternatives, and our discussion of alternatives below, satisfy the RFA. The relevant RFA requirement provides that an IRFA "shall also contain a description of any significant alternatives to the proposed rule which accomplish the

---

554 Proposing Release at 16617 (emphasis added).

555 Proposing Release at 16617-16618. *See also id.* at 16613 ("smaller companies might incur a cost that is disproportionally high, compared to larger companies under the proposed rules").

stated objectives of applicable statutes and which minimize any significant economic impact of the proposed rule on small entities."[556] In the Proposing Release, the Commission discussed each of the types of significant alternatives noted in Section 603 of the RFA and concluded that none of these alternatives would accomplish the stated objectives of the rulemaking while minimizing any significant impact on small entities. In addition, Section III.E of the Proposing Release discussed reasonable alternatives to the proposed rules and their economic impacts. Similarly, in addition to the discussion in Section VI.E below, in Section IV.E of this release we also discuss reasonable alternatives of the final rules and their economic impacts.

While not commenting on the alternatives raised in the IRFA specifically, two commenters stated that the final rules should exempt smaller businesses. One of these commenters stated that small companies in the biotechnology industry "do not have the capacity, nor the business need, to have institutional structures related to the management, planning, oversight, and maintenance of cybersecurity related systems and suppliers. These companies should not have to hire extra employees specifically for the purposes of implementing cybersecurity related programs."[557] The other commenter noted that, with respect to the proposed requirement to require disclosure about the cybersecurity expertise of board members, small companies "have limited resources to begin with, and may find it more difficult than large companies to identify board members with requisite cyber expertise given that there already is a lack of talent in this area."[558]

With respect to the first of these commenters, we note that neither the proposed nor the final rules require any company to "implement new management structures" or otherwise adopt

---

[556] 5 U.S.C. 603(c).

[557] *See* letter from BIO.

[558] *See* letter from NDIA.

or change "institutional structures related to the management, planning, oversight, and maintenance of cybersecurity related systems and suppliers."[559] The final rules instead call for disclosure of a registrant's processes, *if any*, for assessing, identifying, and managing material cybersecurity risks. To the extent that a registrant does not have such processes, the final rules do not impose any additional costs. With respect to the second of these commenters, we note that, consistent with commenter feedback and for the reasons discussed above, we have not adopted the proposed requirement related to disclosure of board cybersecurity expertise.

Finally, we note that many commenters explicitly opposed exempting smaller businesses from the proposed rules,[560] in part because they may face equal[561] or greater[562] cybersecurity risk than larger companies, or because investors' relative share in a smaller company may be higher, such that small companies' cybersecurity risk "may actually embody the most pressing cybersecurity risk to an investor."[563] We agree with these analyses,[564] and accordingly are not exempting small entities from the final rules. However, as discussed above, in response to concerns about the impact of the rules on smaller companies and in order to provide smaller

---

559 The quoted language is from the BIO letter.

560 *See* letters from CSA; Cybersecurity Coalition; NASAA; Prof. Perullo; Tenable.

561 *See* letter from Cybersecurity Coalition.

562 *See* letters from NASAA and Tenable.

563 *See* letter from Prof. Perullo.

564 We note that one commenter stated its conclusion that "cyberattacks mainly affect larger companies." *See* letter from BIO. The basis of the commenter's assertion is that mean market capitalization of impacted companies in the relevant study cited in the Proposing Release is $58.9 billion (Kamiya, et al. (2021)), which it notes is much higher than the average for small companies, and thus concludes that "cyberattacks mainly affect large companies and are not material for smaller companies." As noted in Section IV, *supra*, an average market capitalization of $58.9 billion does not preclude the existence of numerous companies much smaller (and larger) than that amount. *See supra* note 478. The commenter additionally notes that the relevant study states that "firms are more likely to experience cyberattacks when they are larger." To the extent that smaller entities face fewer cyber incidents, that would result in a less frequent need to analyze whether disclosure of such incidents is required under the final rules. However, even if smaller entities are less likely to experience a cyberattack, this would not negate the analysis that such attacks, when they do occur, are more likely to be material for the reasons discussed above.

reporting companies with additional time to prepare to comply with the incident disclosure requirements, we are providing such registrants with an additional 180 days from the non-smaller reporting company compliance date before they must comply with the new Form 8-K requirement.

C. Small Entities Subject to the Final Amendments

The final amendments would apply to registrants that are small entities. The RFA defines "small entity" to mean "small business," "small organization," or "small governmental jurisdiction."[565] For purposes of the RFA, 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.[566] An investment company, including a business development company,[567] 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.[568] We estimate that, as of December 31, 2022, there were approximately 800 issuers and 10 business development companies that may be considered small entities that would be subject to the final amendments.

D. Projected Reporting, Recordkeeping, and other Compliance Requirements

Per the final rules, registrants will be required to report material cybersecurity incidents on Form 8-K and Form 6-K for FPIs, and will be required to describe in their annual reports on Forms 10-K and 20-F certain aspects of their cybersecurity risk management, strategy, and

---

565 5 U.S.C. 601(6).

566 *See* 17 CFR 240.0-10(a) [Exchange Act Rule 0-10a)].

567 Business development companies 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 through 64].

568 17 CFR 270.0-10(a).

governance, if any. The final amendments are described in more detail in Section II above. These requirements generally will apply to small entities to the same extent as other entities, irrespective of size or industry classification, although we are adopting a later compliance date for smaller reporting companies in response to concerns raised by commenters. We continue to expect that the nature of any benefits and costs associated with the amendments to be similar for large and small entities, and so we refer to the discussion of the amendments' economic effects on all affected parties, including small entities, in Section IV above. Also consistent with the discussion in Sections II and IV above, we acknowledge that, in particular to the extent that a smaller entity would be required to provide disclosure under the final rules, it may face costs that are proportionally greater as they may be less able to bear such costs relative to larger entities. However, as discussed in in Section IV, 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, including whether the company actively manages material cybersecurity risks, which makes it difficult to project the economic impact on small entities with precision. To the extent that the disclosure requirements have a greater effect on small registrants relative to large registrants, they could result in adverse effects on competition. The fixed component of the legal costs of preparing the disclosure would be a primary contributing factor. Compliance with certain provisions of the final amendments may require the use of professional skills, including legal, accounting, and technical skills.

E. Agency Action to Minimize Effect on Small Entities

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

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

The rules are intended to better inform investors about cybersecurity incidents and, if any, the cybersecurity risk management, strategy, and governance of registrants of all types and sizes that are subject to the Exchange Act reporting requirements. We explain above in Sections II and IV that current requirements and guidance are not yielding uniform, comparable disclosure sufficient to meet investors' needs. The disclosure that does exist is scattered in various parts of registrants' filings, making it difficult for investors to locate, analyze, and compare across registrants. Staff has also observed that smaller reporting companies generally provide less cybersecurity disclosure as compared to larger registrants, and commenters agreed that there is a need for cybersecurity disclosure from small companies.[569]

Given the current disclosure landscape, exempting small entities or otherwise clarifying, consolidating, or simplifying compliance and reporting requirements under the rules for small entities would frustrate the rulemaking's goal of providing investors with more uniform and timely disclosure about material cybersecurity incidents and about cybersecurity risk management, strategy, and governance practices across all registrants. That said, as discussed in Section II above, we have consolidated and simplified the disclosure requirements for all entities, which should ease small entities' compliance as well. Further, as noted above, smaller

[569] *See supra* notes 339 to 342 and accompanying text.

companies may face equal or greater cybersecurity risk than larger companies, making the disclosures important for investors in these companies.

On the other hand, we believe the rulemaking's goals can be achieved by providing smaller reporting companies with additional time to come into compliance. Therefore, we are delaying smaller reporting companies' required compliance date with the Form 8-K incident disclosure requirement by an additional 180 days from the non-smaller reporting company compliance date. This delay will benefit smaller reporting companies both by giving them extra time to establish disclosure controls and procedures and by allowing them to observe and learn from best practices as they develop among larger registrants.

Similarly, the final rules incorporate a combination of performance and design standards with respect to all subject entities, including small entities, in order to balance the objectives and compliance burdens of the rules. While the final rules do use design standards to promote uniform compliance requirements for all registrants and to address the concerns underlying the amendments, which apply to entities of all size, they also incorporate elements of performance standards to give registrants sufficient flexibility to craft meaningful disclosure that is tailored to their particular facts and circumstances. For example, the final rules require a registrant to describe its "processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes." The rule also provides a non-exclusive list of disclosure items that a registrant should include in providing responsive disclosure to this performance standard; this design element provides registrants with additional guidance with respect to the type of disclosure topics that could be covered and promotes consistency.

Statutory Authority

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

Text of Amendments

For the reasons set forth in the preamble, the Commission amends 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, 78*o*, 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, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that

jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Cybersecurity threat means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Information systems means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

(b) *Risk management and strategy.* (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

(i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;

(ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and

(iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

(2) Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially

affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.

(c) *Governance*. (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.

(2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

(i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

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

(iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Instruction 1 to Item 106(c): 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.

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

(d) *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 § 229.601 by revising paragraph (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; and

* * * * *

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

4. 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), 78*l*, 78m, 78n, 78*o*(d), 78w(a), 78*ll*, 80a-6(c), 80a-8, 80a-29, 80a-30, 80a-37, 80b-4, 80b-6a, 80b-10, 80b-11, 7201 *et seq*.; and 18 U.S.C. 1350, unless otherwise noted.

* * * * *

5. Amend § 232.405 by adding paragraph (b)(4)(v) to read as follows:

§ 232.405 Interactive Data File submissions.

* * * * *

(b) * * *

(4) * * *

(v) Any disclosure provided in response to: §229.106 of this chapter (Item 106 of Regulation S-K); Item 1.05 of §249.308 of this chapter (Item 1.05 of Form 8-K); and Item 16K of § 249.220f of this chapter (Item 16K of Form 20-F).

* * * * *

PART 239—FORMS PRESCRIBED UNDER THE SECURITIES ACT OF 1933

6. The general authority citation for part 239 continues to read as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s, 77z–2, 77z–3, 77sss, 78c, 78*l,* 78m, 78n, 78*o*(d), 78*o*–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, 80a–37, and sec. 71003 and sec. 84001, Pub. L. 114–94, 129 Stat. 1321, unless otherwise noted.

* * * * *

7. 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

* * * * *

8. Amend Form S-3 (referenced in § 239.13) by adding General Instruction I.A.3(b).

Note: Form S-3 is attached as Appendix A to this document. Form S-3 will not appear in the Code of Federal Regulations.

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

9. 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, 78j–4, 78k, 78k–1, 78*l,* 78m, 78n, 78n–1, 78*o,* 78*o*–4, 78*o*–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, 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; and 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.

* * * * *

10. 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.

11. 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

12. 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 249.310 is also issued under secs. 3(a), 202, 208, 302, 406 and 407, Pub. L. 107–204, 116 Stat. 745.

* * * * *

13. Revise Form 20-F (referenced in § 249.220f) by adding Item 16K.

Note: Form 20-F is attached as Appendix B to this document. Form 20-F will not appear in the Code of Federal Regulations.

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

15. Revise Form 8-K (referenced in § 249.308) by:

a. Revising General Instruction B.1.;

b. Revising General Instruction G.1.; and

c. Adding Item 1.05.

Note: Form 8-K is attached as Appendix C to this document. Form 8-K will not appear in the Code of Federal Regulations.

16. Revise Form 10-K (referenced in § 249.310) by:

a. Revising General Instruction J(1)(b); and

b. Adding Item 1C to Part I.

Note: Form 10-K is attached as Appendix D to this document. Form 10-K will not appear in the Code of Federal Regulations.

* * * * *

By the Commission.

Dated: July 26, 2023.

Vanessa A. Countryman,

Secretary.

Note: The following appendices will not appear in the Code of Federal Regulations.

Appendix A—Form S-3

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. * * *

(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.

* * * * *

Appendix B—Form 20-F

FORM 20-F

* * * * *

PART II

* * * * *

Item 16K. Cybersecurity.

(a) Definitions. For purposes of this section:

(1) *Cybersecurity incident* means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

(2) *Cybersecurity threat* means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

(3) *Information systems* means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

(b) Risk management and strategy. (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail

for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

(i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;

(ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and

(iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

(2) Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.

(c) *Governance*. (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.

(2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

(i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

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

(iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Instructions to Item 16K(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 expertise of management in paragraph (c)(2)(i) of this Item may include, for example: Prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.

(d) *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 16K. Item 16K applies only to annual reports, and does not apply to registration statements on Form 20-F.

* * * * *

Appendix C—Form 8-K

FORM 8-K

* * * * *

GENERAL INSTRUCTIONS

* * * * *

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.

* * * * *

G. Use of this Form by Asset-Backed Issuers.

* * * * *

1. * * *

(a) Item 1.05, Cybersecurity Incidents;

(b) Item 2.01, Completion of Acquisition or Disposition of Assets;

(c) Item 2.02, Results of Operations and Financial Condition;

(d) Item 2.03, Creation of a Direct Financial Obligation or an Obligation under an Off-Balance Sheet Arrangement of a Registrant;

(e) Item 2.05, Costs Associated with Exit or Disposal Activities;

(f) Item 2.06, Material Impairments;

(g) Item 3.01, Notice of Delisting or Failure to Satisfy a Continued Listing Rule or Standard; Transfer of Listing;

(h) Item 3.02, Unregistered Sales of Equity Securities;

(i) Item 4.01, Changes in Registrant's Certifying Accountant;

(j) Item 4.02, Non-Reliance on Previously Issued Financial Statements or a Related Audit Report or Completed Interim Review;

(k) Item 5.01, Changes in Control of Registrant;

(*l*) Item 5.02, Departure of Directors or Principal Officers; Election of Directors; Appointment of Principal Officers;

(m) Item 5.04, Temporary Suspension of Trading Under Registrant's Employee Benefit Plans; and

(n) Item 5.05, Amendments to the Registrant's Code of Ethics, or Waiver of a Provision of the Code of Ethics.

* * * * *

INFORMATION TO BE INCLUDED IN THE REPORT

Section 1 – Registrant's Business and Operations

* * * * *

Item 1.05 Material Cybersecurity Incidents.

(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.

(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.

(c) Notwithstanding General Instruction B.1. to Form 8-K, if the United States Attorney General determines that disclosure required by paragraph (a) of this Item 1.05 poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, the registrant may delay providing the disclosure required by this Item 1.05 for a time period specified by the Attorney General, up to 30 days following the date when the disclosure required by this Item 1.05 was otherwise required to be provided. Disclosure may be delayed for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay under this paragraph, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order.

(d) Notwithstanding General Instruction B.1. to Form 8-K, if a registrant that is subject to 47 CFR 64.2011 is required to delay disclosing a data breach pursuant to such rule, it may delay providing the disclosure required by this Item 1.05 for such period that is applicable under 47 CFR 64.2011(b)(1) and in no event for more than seven business days after notification required under such provision has been made, so long as the registrant notifies the Commission in correspondence submitted to the EDGAR system no later than the date when the disclosure required by this Item 1.05 was otherwise required to be provided.

Instructions to Item 1.05.

1. A registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident.

2. To the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the registrant shall include a statement to this effect in the filing and then must file an amendment to its Form 8-K filing under this Item 1.05 containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.

3. The definition of the term "cybersecurity incident" in §229.106(a) [Item 106(a) of Regulation S-K] applies to this Item.

4. A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.

* * * * *

Appendix D—Form 10-K

FORM 10-K

* * * * *

GENERAL INSTRUCTIONS

* * * * *

J. Use of this Form by Asset-Backed Issuers.

* * * * *

(1) * * *

(b) Item 1A, Risk Factors and Item 1C, Cybersecurity;

* * * * *

Part I

* * * * *

Item 1C. Cybersecurity.

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

* * * * *