May 9, 2022

Via Email

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
Release Nos. 33-11038, 34-94382; File No. S7-09-22

Dear Ms. Countryman:

We write on behalf of the American Gas Association ("AGA") and the Interstate Natural Gas Association of America ("INGAA") to provide feedback regarding the Securities and Exchange Commission's (the "Commission") proposed rule governing disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies subject to the reporting requirements of the Securities Exchange Act of 1934 (the "Exchange Act"). As discussed below, while AGA and INGAA appreciate the rationale behind the Commission's proposed rule, we believe that the current proposal should be modified to reflect longstanding concepts of materiality and to reduce the risk of inadvertently exposing issuers to cybersecurity threats. AGA and INGAA therefore respectfully request that the Commission revise the proposed amendments to incorporate and account for the comments below.

AGA represents more than 200 energy companies that deliver clean natural gas throughout the United States. The majority of the AGA's members issue common stock that is registered under Section 12(b) of the Exchange Act, and traded on the New York Stock Exchange, the Nasdaq, and other U.S. securities exchanges. AGA's mission is to facilitate, on its members' behalf, the promotion of safe, reliable, and efficient delivery of natural gas to homes and businesses across the nation. AGA's members include U.S. energy utilities, transmission and marketing companies, exploration and production companies, products and services companies, international energy companies and affiliates, and industry associates.

INGAA represents the U.S. natural gas pipeline industry. INGAA's members deliver clean, abundant, and affordable natural gas throughout North America and operate approximately 200,000 miles of pipelines that serve as an indispensable link between natural gas producers and consumers.

The Proposed Amendments Should Comport with Longstanding Concepts of Materiality

As the Commission recognizes,[1] it is well established that the materiality framework governs

[1] *See* SEC Release Nos. 33-11038, 34-94382, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, File No. S7-09-22 ("Release") at 22-23.

disclosure under the securities laws.[2] Although there are different articulations of the materiality standard, public companies are required to disclose information for which "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have 'significantly altered the "total mix" of information made available.'"[3] Relatedly, the Commission, its staff, and the courts have recognized that the materiality assessment generally requires both a quantitative and qualitative analysis.[4] On several occasions prior to the issuance of the current proposed rule, the Commission and its staff have applied the general materiality standard to assess disclosure obligations regarding threats to cybersecurity and digital infrastructure.[5]

The proposed rule should not alter this longstanding materiality framework, and we suggest that the Commission's final rule explicitly affirm the application of decades of materiality-related precedent and guidance to cybersecurity risks and incidents.[6] We believe that the existing authoritative guidance provides an adequate framework for public companies that are victims of cyber incidents to evaluate their disclosure obligations to investors.[7] That guidance instructs issuers to evaluate, for example, the impact of an incident on revenue and net income, whether the risk or incident affects the company's compliance with other regulatory or contractual

---

[2] *See, e.g.*, Exchange Act, Section 18(a), 15 U.S.C. § 78r(a) ("Any person who shall make or cause to be made any statement in any application, report, or document . . . which statement was at the time and in the light of the circumstances under which it was made false or misleading with respect to any material fact, shall be liable . . . ."); *Basic Inc. v. Levinson*, 485 U.S. 224, 240 (1988) ("[M]ateriality depends on the significance the reasonable investor would place on the withheld or misrepresented information."); *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1977) ("[A]n omitted fact is material if there is a substantial likelihood that a reasonable investor would consider it important in deciding how to vote. . . . Put another way, there must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available.").

[3] Release at 23 (quoting *TSC Indus.*, 426 U.S. at 449).

[4] SEC Staff Accounting Bulletin 99.

[5] *See, e.g.*, SEC, Division of Corporate Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011) (in the context of increased use of digital technologies); *cf.* SEC, Statement of the Commission Regarding Disclosure of Year 2000 Issues, Release No. 34-40277 (Aug. 4, 1998) (in the context of the anticipated Year 2000 bug).

[6] *See, e.g.*, Securities Act of 1933 (adopting materiality standard at Section 17(a)(2)); Securities Exchange Act of 1934 (adopting materiality standard at Section 18(a)); *TSC Indus.*, 426 U.S. 438 (articulating materiality standard in 1976); BUSINESS ROUNDTABLE, THE MATERIALITY STANDARD FOR PUBLIC COMPANY DISCLOSURE: MAINTAIN WHAT WORKS 14 (2015), available at https://s3.amazonaws.com/brt.org/archive/reports/BRT.The%20Materiality%20Standard%20for%20Public%20Company%20Disclosure.2015.10.29.pdf [hereinafter "BUSINESS ROUNDTABLE"] ("For more than eight decades, the materiality principle has governed public company disclosure under the federal securities laws . . . .").

[7] *See Basic*, 485 U.S. at 236 (explaining that determination of materiality is an "inherently fact-specific finding"); SEC Accounting Bulletin 99 ("[A]n assessment of materiality requires that one views the facts in the context of the 'surrounding circumstances,' . . . or the 'total mix' of information . . . ."); BUSINESS ROUNDTABLE, supra note 6 at 6 (noting materiality "benefits investors in three ways": by ensuring investors are not "buried in an avalanche of trivial information"; by requiring public companies to consider disclosure based on "their particular facts and circumstances"; and by allowing companies to adjust their disclosures based on changes in the economy or within a public company affecting what information would be important to a reasonable disclosure).

requirements, and any other factor that may impact the "total mix" of information.[8] In addition, the Commission's recent enforcement actions against issuers that failed to disclose material cybersecurity incidents make clear that the materiality of an incident depends in part on the nature of the registrant's business.[9]

Collectively, the guidance issued by the Commission and Courts for over thirty years since the Supreme Court articulated the *Basic v. Levinson* standard provides companies with ample guidance to assess materiality of cybersecurity incidents. Any deviation from the existing longstanding framework would create confusion where none currently exists, and ultimately frustrate one of the Commission's primary objectives behind the proposed rulemaking—i.e., to ensure that investors receive information important enough to evaluate the risks of an investment.[10] For those reasons, AGA and INGAA support the continued application of longstanding materiality principles to cybersecurity incidents and risks.

Requiring Disclosure of All Incidents that Lead to
Policy Changes Is Inconsistent with the Materiality Standard

The proposed rule would require registrants to disclose any cyber incidents that lead to changes in the company's policies and procedures, even where the underlying cyber incidents are entirely immaterial.[11] We oppose this proposal, which would effectively mandate disclosure of numerous inconsequential cybersecurity incidents and thereby effectively override the longstanding materiality standard (discussed above) and potentially "bury investors in an avalanche of trivial [and confusing] information."[12] Moreover, the proposed rule would actually disincentivize companies from proactively improving their cyber policies, procedures, systems, and controls by mandating disclosure of meaningless cyber incidents that could be linked—however remotely—to those improvements. We believe that in assessing the contours of any mandated cyber disclosures, including those that result in changes to policies and procedures, the Commission should continue to be guided by materiality.

---

[8] SEC Staff Accounting Bulletin 99.

[9] *See, e.g.*, *In the Matter of Pearson, plc*, A.P. File No. 3-220462, Sec. Exchange Act Release No. 92676 (Aug. 16, 2021) (finding PII-related breach to be material because respondent's business "involved collection and storage of large quantities of private data.").

[10] *See* Release at 55 (citing 15 USC § 77(b)(b); 15 USC § 78(c)(f)) (noting the statutory requirement that the Commission must consider whether proposed rulemaking "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.").

[11] *See* Release at 38 (noting that Form 106(b) requires disclosure of cybersecurity related risks and incidents that have affected the registrant's results of operations or financial condition and cybersecurity risks that are considered as part of the registrant's business strategy); Release at 106-07 (same).

[12] BUSINESS ROUNDTABLE, supra note 6 at 6.

Requiring Disclosure Regarding Management's Role in Implementing
Cybersecurity Policies Is Too Granular and Not Beneficial to Investors

The Commission should not adopt Item 106(c) as proposed.[13] The details the Commission would potentially require with regard to the description of management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures, and strategies are far too granular to be useful to investors.

With respect to cybersecurity matters, investors expect an overview that provides assurance that management and the board of directors are devoting appropriate attention to issues. Granular details regarding a registrant's management expertise and oversight regarding the registrant's policies, procedures, strategies, and incident responses are not beneficial to making investment decisions. This granular detail is also subject to frequent change including based on developments in technology and management practices.

To account for those realities, we suggest the following modification to proposed Item 106(c)(2):

> Describe whether registrant has a designated chief information security officer, or someone in a comparable position, and whether and how frequently such person reports to the board of directors or a committee of the board of directors regarding cybersecurity risk.

This information should be sufficient for investors to make a determination regarding whether management and the board of directors are paying appropriate attention to cybersecurity issues. Additional information is not necessary for investors and puts the Commission in the position of regulating a registrant's policies, procedures, and strategies instead of its disclosures.

In conformity with the suggested modification above to proposed Item 106(c)(2), and for the same reasons as stated above, the Commission should modify proposed Item 407(j)(1)[14] to contain solely the same language as the suggested modification above to proposed Item 106(c)(2).

The Commission Should Not Require Companies to Make
Disclosures Prior to the Completion of Materiality Assessments

The Commission seeks comments regarding whether there should be "a different triggering event for the Item 1.05 disclosure, such as the registrant's discovery that it has experienced a cybersecurity incident, even if the registrant has not yet been able to determine the materiality of the incident."[15] Because this proposed requirement, if adopted, is likely to confuse investors, lead to duplicative—and potentially contradictory—disclosures, and frustrate the ability of victims of cybersecurity incidents to conduct appropriate investigations, AGA and INGAA believe that this proposal is inconsistent with the Exchange Act and the Commission should decline to adopt it.

---

[13] *See* Release at 42.

[14] *See* Release at 46.

[15] *See* Release at 29.

Importantly, a company's understanding regarding the facts and circumstances of a cyber incident may differ **materially** when an incident is initially discovered and when the company subsequently makes a materiality determination. If disclosure is required both upon discovery of the incident and again upon a materiality determination, companies will inevitably disclose numerous immaterial incidents.

The Commission should allow companies to delay disclosure of cybersecurity incidents in the event of an ongoing internal investigation so long as the investigation is completed without undue delay. A specific timeframe for reporting that is unrelated to the completion of a materiality determination is arbitrary and capricious. By contrast, AGA and INGAA's proposed undue delay standard would permit companies to gather and analyze all facts necessary for making a materiality determination. Forcing a materiality determination while the company is taking these steps will undoubtedly pull important resources away from necessary response activities (which could ultimately harm investors). Importantly, disclosure prior to these steps and making this determination is also likely to lead to inaccurate materiality determinations, which will create information uncertainty and cause undue alarm to investors.

Additionally, where cybersecurity incidents are determined to be material, the two sets of disclosures that companies will be required to make may vary from each other in important respects. Accordingly, a proposed early disclosure requirement, which is inconsistent with the foundational principle of U.S. securities regulation that disclosure is premised upon materiality, will shift the burden to investors to sift through multiple sets of (unnecessary) disclosures. For those reasons, the Commission should not require issuers to make any disclosures prior to a materiality determination.[16]

The Commission's consideration of a requirement that companies disclose cyber incidents when they are initially discovered appears to be premised upon the belief that registrants may delay completing materiality determinations to avoid making timely disclosures.[17] AGA and INGAA believe that this risk is low for two reasons. *First*, AGA and INGAA believe that existing operational, cybersecurity, and financial realities already incentivize companies to investigate expeditiously cyber incidents. *Second*, to the extent an issuer fails to timely evaluate whether a cybersecurity incident is material, the Commission already has tools in place to hold those companies accountable, including Exchange Act Rule 13a-15(a), which requires public companies to maintain disclosure controls and procedures designed to ensure that material information is disclosed to investors in a timely manner.[18]

Relatedly, the Commission also seeks comments regarding the timing and form of disclosures in the event that a company determines that "a series of previously undisclosed individually

[16] *See* Release at 30; Release at 127 (Instructions to Item 1.05).

[17] *See* Release at 31.

[18] *See* Rule 13a-15(a), (e); *see also In the Matter of First Am. Fin. Corp.*, A.P. File No. 3-20367, Sec. Exchange Act Release No. 92176 (June 14, 2021) (enforcement action based on insufficient disclosure controls and procedures premised on respondent's failure to evaluate timely whether to disclose cyber breach).

immaterial cybersecurity incidents becomes material in the aggregate."[19] Under these circumstances, AGA and INGAA believe that the timeline for reporting should begin to run as of the materiality determination related to the final incident—i.e., when the company determines that the incidents in the aggregate constitute a material event. The Commission also proposes to require registrants to disclose details related to the individually immaterial cybersecurity incidents when they become material in the aggregate.[20] But providing detailed disclosure of each immaterial incident would be inconsistent with the general materiality standard and could provide potential threat actors with information regarding a company's vulnerabilities (without any corresponding benefit to investors). Issuers should therefore only be required to disclose information regarding these immaterial incidents to the extent that such information is necessary for investors to be fully informed regarding the aggregate material impact.

For those reasons, AGA and INGAA support the Commission's position that the proposed four-day disclosure window, if implemented, should not be triggered until the date that a registrant determines that a cybersecurity incident—or combination of incidents—is material.[21] Disclosure should not be based upon the registrant's mere discovery that it has experienced a cybersecurity event prior to an assessment of materiality.[22] Finally, when a combination of individually immaterial incidents becomes material in the aggregate, disclosures regarding those individual incidents should be required only as they relate to the aggregate material impact.

Increasing the Level of Required Detail in Disclosures
Could Expose Companies to Additional Cyber Threats

The Commission has requested comments regarding whether the substance or timing of the proposed disclosures may "have the unintentional effect of putting registrants at additional risk of future cybersecurity incidents."[23] AGA and INGAA believe that this is a meaningful risk and suggest that the Commission amend certain proposed requirements to mitigate its potential impact.

In particular, AGA and INGAA suggest that proposed Items 1.05, 106(b), and 106(c)(2) should be modified to provide that the required disclosures may be high-level in nature and that registrants may consider, in determining the appropriate level of detail, whether providing certain information may constitute an independent security risk. For example, proposed Item 1.05(5) would require the registrant to disclose whether it has remediated or is currently remediating a cybersecurity incident. If a registrant is currently remediating an incident, the incident may be ongoing and disclosure of that fact may encourage additional malicious acts. Indeed, the Commission acknowledges that, under certain circumstances, timely disclosure exposes registrants'

[19] *See* Release at 31.

[20] Release at 33-34.

[21] *See* Release at 22.

[22] AGA also notes that the process of investigating a cybersecurity incident and applying the available materiality guidance to the facts and circumstances may be time consuming, and often requires coordination with counsel, auditors and accountants, and cybersecurity consultants. Any rulemaking that impacts the timing of required disclosures should be mindful of that reality.

[23] *See* Release at 29; 43.

vulnerabilities to malicious actors who could even "exacerbate an ongoing attack" using the disclosed information.[24] The risk associated with disclosure of excessive details may also create a chilling effect on registrants' willingness to disclose cybersecurity incidents.

For those reasons, AGA and INGAA suggest that proposed Items 1.05, 106(b), and 106(c)(2) be modified to provide that the required disclosures may be high-level in nature and that registrants may consider the cybersecurity risk associated with disclosing additional details in determining whether they are required to do so. AGA and INGAA note that this proposed modification is consistent with the disclosure regimes of many states, which generally require public companies to disclose these items at a high level. Additionally, AGA and INGAA suggest that registrants be permitted to delay disclosure as necessary to determine the scope of an incident and restore the reasonable integrity of any compromised systems.

The Commission Should Not Require Disclosure of Information
that Could Undermine Ongoing Law Enforcement Investigations

The Commission has requested comments regarding whether registrants should be allowed to "delay reporting of a cybersecurity incident where the Attorney General requests such a delay … in the interest of national security."[25] AGA and INGAA agree with this proposal and suggest that the Commission expand the circumstances under which companies may delay reporting to include any cybersecurity incident for which a law enforcement agency concludes that disclosure would undermine an ongoing criminal or civil investigation. Allowing issuers to delay reporting—particularly in response to specific requests from law enforcement—may facilitate investigations aimed at apprehending threat actors, which may, in turn, prevent further cybersecurity incidents (thereby protecting investors).

***

AGA and INGAA appreciate the Commission's overall objective behind the proposed rulemaking. Pursuant to longstanding principles of securities regulation in the United States, public companies should be required to disclose material cyber incidents and risks to investors. The comments in this correspondence are designed to bring the Commission's proposal into alignment with that bedrock principle and prevent companies from being forced to disclose information that could lead to additional cybersecurity incidents and ultimately frustrate the Commission's investor protection mandate.[26]

We thank the Commission for considering our perspective on these important issues.

[24] Release at 75.

[25] Release at 30.

[26] About the SEC, What we do, available at https://www.sec.gov/Articule/whatwedohtml (explaining the Commission's three-part mandate).

Sincerely,

Kimberly Denbow
Managing Director, Security & Operations
American Gas Association

Amy Andryszak
Chief Executive Officer
Interstate Natural Gas Association of America