



**Mary A. Francis**  
Corporate Secretary and Chief Governance Officer

May 6, 2022

**Via E-mail to rule-comments@sec.gov**

Vanessa A. Countryman  
Secretary  
U.S. Securities and Exchange Commission  
100 F Street NE  
Washington, DC 20549-1090

**Re: Proposing Release – Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, File No. S7-09-22**

Chevron Corporation (“Chevron”, “the Company”, or “we”) appreciates the opportunity to provide comments in response to the U.S. Securities and Exchange Commission (the “Commission” or “SEC”) proposed rule on *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, issued on March 9, 2022 (the “Proposing Release”).

Chevron is one of the world’s leading integrated energy companies. Through its subsidiaries that conduct business worldwide, the Company is involved in virtually every facet of the energy industry.

Chevron supports the Commission’s goals of improving the availability of consistent, comparable, and decision-useful disclosures by public companies about their cybersecurity risk management, strategy, and governance practices. For the reasons we discuss further in this letter, we are concerned that certain aspects of the Proposing Release would not satisfy this objective and would instead provide information to investors that is not decision-useful, while creating security concerns for registrants.

**Current disclosure of material cybersecurity incidents on Form 8-K**

**Materiality trigger and associated safeguards**

Chevron agrees with the Commission that companies should not be required to report cybersecurity incidents prior to management’s determination of their materiality.<sup>1</sup> The substantial majority of cyber threats against companies do not have significant impact, and disclosure of such incidents, versus those identified as material, would inundate investors with inconsequential information.

The Company also supports the Commission’s proposed approach to include Form 8-K Item 1.05 in the Exchange Act Rules 13a-11 and 15d-11 safe harbors. Given the stealth nature of cybersecurity incidents, the proposed strict timing requirements of Form 8-K Item 1.05, and the related materiality determinations required, there is increased risk that the question of whether a material cybersecurity incident disclosure was timely made under proposed Item 1.05, as well as management’s materiality determination itself, would be second-guessed and potentially challenged by investors and others.

We believe that the foregoing considerations, coupled with the proposed requirement to make a materiality determination for an incident “as soon as reasonably practicable” after its discovery, warrant safe harbor protection. For the same reasons, the Company supports the Commission’s proposed approach

---

<sup>1</sup> We refer to the traditional materiality standard anchored in *Basic, Inc. v. Levinson*, 485 U.S. 224, 232 (1988).

that the failure to timely file a Form 8-K under Item 1.05 would not result in the loss of the registrant's eligibility to file a registration statement on Form S-3. The Company further encourages the Commission to permit registrants to furnish, rather than requiring them to file, an Item 1.05 Form 8-K. Consistent with statements of a former Co-Director of the Division of Enforcement, we also ask for the Commission's final rule to "recognize this is a complex area subject to significant judgment, and [the Commission is] not looking to second-guess reasonable, good faith disclosure decisions."<sup>2</sup>

In addition, the Company believes a safe harbor should be available for information about cybersecurity incidents affecting systems used but not owned by a registrant. Although the terms of such arrangements generally require the third-party service provider to implement security measures, registrants, including Chevron, may not have ready access to information about cybersecurity incidents affecting third-party systems, including the fact that an incident has occurred, that would be necessary to assess materiality. We believe any safe harbor for third-party systems should still require registrants to assess materiality to the registrant of any known cybersecurity incident affecting the third-party system that the registrant uses. Otherwise, investors would not receive potentially material information about cybersecurity risks or exposures from registrants that use public cloud services or other third-party systems.

*Reporting delay when there is cooperation with law enforcement or other government agencies, ransomware involved, or an ongoing internal investigation that would be jeopardized*

We urge the Commission to consider a revision to the proposed rule to allow an exception that permits additional time to report a cybersecurity incident in certain circumstances. Such delay may be warranted when a registrant is cooperating with or taking directions from law enforcement or other government agencies in connection with the incident. These circumstances include, for example, when a registrant is cooperating with law enforcement to assist in the apprehension of the perpetrators of a cybersecurity incident, negotiating with a threat actor to recover critical corporate assets affected by a ransomware attack, or conducting an internal investigation (particularly at the stage of the investigation where disclosing details of a cyber incident externally may increase the company's vulnerability to malicious acts or exploitation while the incident has not been fully remediated). In these circumstances, a premature disclosure of the incident may put at risk the company's ongoing efforts to detect the wrongdoers, recover corporate assets, or block harmful cyber activity against the company through exploitation of an identified vulnerability, which ultimately would harm investors.

Further, the required timeline for proposed Form 8-K Item 1.05 disclosure may undermine other government agencies' efforts to address cybersecurity attacks. For example, the Cyber Incident Reporting for Critical Infrastructure Act, enacted in March 2022, requires owners and operators of critical infrastructure to report certain cyber incidents to the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours after an incident is reasonably confirmed, and any ransomware payments within 24 hours after the payment is made. These disclosure rules are intended in part to allow CISA and other agencies to gather information about the incidents and distribute security alerts if they involve vulnerabilities that pose risks to other companies. Notably, to our knowledge, no state or federal law requires *public* disclosure of a cyber incident immediately or shortly after its discovery. Forcing early market disclosure of a cyber incident, such as those contemplated by the

---

<sup>2</sup> See "The SEC Enforcement Division's Initiatives Regarding Retail Investor Protection and Cybersecurity" (October 26, 2017), available at <https://www.sec.gov/news/speech/speech-avakian-2017-10-26>.

proposed Form 8-K Item 1.05, may undermine other government agencies' efforts to address and protect critical infrastructure.

*Content of proposed Form 8-K Item 1.05*

Chevron believes the scope of the proposed contents of Form 8-K Item 1.05 should remain limited to general information, as proposed, and not include specific or technical information or other details that may impede the registrant's response or remediation of the incident, such as the list of vendors the registrant is using, the identity of the actor, or the origin of the attack. Beyond complicating incident response, detailed information regarding an incident would not provide additional benefit to investors.

**Disclosure of updates about material cybersecurity incidents on Forms 10-Q and 10-K**

Regarding the requirement in the Proposing Release to determine whether a series of previously undisclosed individually immaterial cybersecurity incidents have become material in the aggregate, the Proposing Release's description of such aggregation appears vague and difficult to operationalize. For instance, under the proposed requirement, it is not clear whether a registrant should aggregate the same types of incidents, multiple incidents from the same attacker, attacks across different geographies, or attacks within a specific timeframe. Further, it is unclear how such aggregated information would be beneficial to investors' understanding of a registrant's business and cybersecurity risk management. The SEC's provision of additional guidance and parameters on the proposed aggregation requirement would help registrants comply and promote consistent disclosure standards for the benefit of investors.

**Disclosure of cybersecurity risk management, strategy, and governance**

Chevron believes that the broad scope of disclosure requirements under proposed Regulation S-K Items 106(b) and 106(c) would result in lengthy disclosures that are not necessarily useful to investors but could serve as a roadmap for potential cyber attackers. Any disclosure requirements with respect to registrants' policies and procedures for identifying and managing cybersecurity risks should be narrowly tailored to require a high-level overview rather than specific details of registrants' cybersecurity programs. For example, in response to Question 20 of the Proposing Release, registrants should not be required to identify the third-party entities they use, including any cybersecurity assessor, consultant, auditor, or other service providers. We do not believe such information would be decision-useful for investors, particularly for large companies that rely on different third-party service providers for each major project or joint venture. Moreover, certain third-party services, such as those based on open source software, might be virtually impossible to trace or disclose in an easily-understandable format. Similarly, in response to Question 22 of the Proposing Release, the details of the registrant's incident response processes and techniques, including specific tools, should not be required to be disclosed. Such information could offer a roadmap to potential attackers, in which case the potential harm would clearly outweigh the benefits to investors.

Regarding the proposed definitions under Regulation S-K Item 106(a), these definitions should be consistent with existing comparable definitions used under other federal laws and regulations, to the extent a comparable definition is available, such as the definition of "cybersecurity incident" found in the National Institute of Standards and Technology (NIST) Cybersecurity Framework or the definition of "incident" found in NIST Special Publication 800-37, Appendix B. We also believe the proposed definition of "cybersecurity threat" should be refined with more parameters, including a probability threshold, as certain terms in the proposed definition (such as "any potential occurrence" and "may result in") do not provide instructive boundaries. In addition, we urge the Commission to define the "operational

technology systems” that can cause material cybersecurity incidents in certain industries.<sup>3</sup> 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.

\* \* \*

We hope our comments are helpful to the Commission in determining next steps for this proposed rule. If you have any questions on the content of this letter, please contact me at [REDACTED]

Sincerely,



Mary A. Francis  
Corporate Secretary and Chief Governance Officer

cc: The Honorable Gary Gensler, Chair  
The Honorable Hester M. Peirce, Commissioner  
The Honorable Allison Herren Lee, Commissioner  
The Honorable Caroline A. Crenshaw, Commissioner

---

<sup>3</sup> NIST Special Publication 800-37, Appendix B defines “Operational Technology” as “Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.” Critical Infrastructure organizations rely on Operational Technology systems to operate significant aspects of physical industrial systems, such as pipelines and powerplants.