May 9, 2022

The Honorable Gary Gensler, Chairman Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090
(rule-comments@sec.gov)

VIA EMAIL (rule-comments@sec.gov)

RE: File Number S7-09-22, Comments of the American Petroleum Institute the Association of Oil Pipe Lines and the American Fuel & Petrochemical Manufacturers in Response to Securities and Exchange Commission's Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Chairman Gensler:

The American Petroleum Institute ("API"), the Association of Oil Pipe Lines ("AOPL") and the American Fuel & Petrochemical Manufacturers ("AFPM") respectfully submit these comments on the proposed rule of the Securities and Exchange Commission ("SEC" or "Commission") regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure ("Proposal"). These organizations represent companies from all segments of the American oil and natural gas industry and are involved in exploration, production, refining, marketing, distribution, and marine activities.

Cybersecurity is an issue of paramount concern to our members and the industry has taken steps and committed resources to the safety and security of our operations. For example, the industry has established multiple Information Sharing and Analysis Centers that are dedicated to the oil and natural gas sector to share cyber threat information and

disseminate mitigation and prevention best practices in a timely manner.[1] Member companies have also instituted highly regarded standards and frameworks to strengthen their cybersecurity posture such as the National Institute for Standards and Technology's ("NIST") Cybersecurity Framework. This framework is widely used within our industry and our members actively participated in its development and updating.[2] API has also written and published an industry standard, API STD 1164, *Pipeline Control Systems Cybersecurity*, to guide companies in strengthening the cybersecurity of pipeline operations.[3] Additionally, the industry works closely with our federal partners—including the Cybersecurity and Infrastructure Security Agency ("CISA") and the Federal Bureau of Investigation ("FBI")—to continuously mitigate new and emerging threats to ensure member companies are prepared for cyber incidents.

We acknowledge the Commission for taking an interest in engaging on this important topic, which has been primarily the province of the Department of Homeland Security ("DHS"), along with the FBI and the other elements of the intelligence community and federal law enforcement. Although there is a role for the Commission regarding how registrants approach communicating cybersecurity risks to investors, we believe that existing Commission guidance adequately protects investors[4] and the Proposal surpasses the Commission's legal authority and presents significant policy concerns that would ultimately harm registrants (and accordingly harm investors) if finalized in its current form. The Proposal, albeit well intentioned, would undermine cybersecurity efforts rather than advance them, and it would impose significant costs on public companies.

---

[1] *See* Oil and Natural Gas Info. Sharing and Analysis Ctr., *Fueling the Exchange of Cyber Intelligence, https://ongisac.org/ (last visited May 9, 2022);* Downstream Natural Gas Info. Sharing and Analysis Ctr., *Mission, https://dngisac.com/ (last visited May 9, 2022)*

[2] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, (April 16, 2018), available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[3] API STD 1164 Pipeline Control Systems Cybersecurity, (3rd Edition, August 2021).

[4] See, SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 1, 12 (Feb. 26, 2018), available at https://www.sec.gov/rules/interp/2018/33-10459.pdf (explaining that companies should provide timely and ongoing information in periodic reports about material cybersecurity risks and incidents that trigger disclosure obligations).

I. Consideration of the Commission's Statutory Authority to Finalize the Proposal.

The Commission's authority to require public disclosures is limited by the statutes that give it rulemaking authority.[5] Although Congress has conferred on the Commission the power to promulgate rules that require public disclosures in both the Securities Act and the Exchange Act,[6] the Proposal could surpass those grants of authority and its mission of protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation.[7]

The Proposal contains only a limited explanation of the statutory authority behind the rulemaking and does not adequately clarify why the robust guidance issued by the Commission in 2018 is inadequate to address the Commission's expressed concern of informing investors of a registrant's approach to cybersecurity risks and the material impacts from cybersecurity events. To ensure our organizations and other stakeholders have such an opportunity to understand the full authority to propose rules beyond what may be relevant or useful to investors, further elaboration of the legal basis for finalizing the rule beyond one passing reference to over 70 pages of statutory text is necessary.

Certainly, the Securities Act and Exchange Act empowers the Commission to require disclosures related to the financial health of a registrant and to give investors a true picture of the securities on the market. Rulemaking in areas beyond this, however, have been limited and are best defined by Congress. For example, Congress has used statutory authorizations to require disclosures on corporate responsibility, corporate governance, and selected aspects of executive compensation.[8] Similarly, Congress has spoken clearly when it previously authorized the Commission to require disclosures related to specific public policy concerns, such as "conflict minerals."[9] This practice is appropriate because

---

[5] *New York Stock Exch. LLC v. SEC*, 962 F.3d 541, 554 (D.C. Cir. 2020).

[6] *See* 15 U.S.C. §§ 77g(a)(1), 77s(a), 78l(b)(1), 78m(a), 78w(a).

[7] *Id.* § 78qq(a)(2)(A). Section 11A of the Exchange Act authorizes the Commission "to facilitate the establishment of a national market system for securities" and "having due regard for the public interest, the protection of investors, and the maintenance of fair and orderly markets, to use its authority" to achieve this goal. *Id.* § 78k-1(a)(2).

[8] *See* SEC, *Concept Release, Business and Financial Disclosure Required by Regulation S-K*, 81 Fed. Reg. 23,916, 23,922 (April 22, 2016).

[9] *See id.* At 23,969-70 (explaining that Section 1502 of the Dodd Frank Act mandated that the Commission adopt rules regarding registrants' use of "conflict minerals."); Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"), 15 U.S.C. § 78m(p) (2010).

it is well established that the courts "expect Congress to speak clearly if it wishes to assign to an executive agency decisions of vast economic and political significance."[10]

With respect to cybersecurity, Congress has not clearly authorized the Commission to promulgate broad regulations requiring registrants to disclose cybersecurity information in their registration statements and quarterly and annual filings, which will impose significant costs upon issuers in their registration statements and quarterly and annual filings. Rather, given that cybersecurity concerns present economic, political, and national security significance, Congress has repeatedly legislated in recent years and assigned new regulatory powers to other agencies—and not the Commission.[11] These enactments have included broad information sharing requirements to facilitate and encourage the private sector to share information with DHS, FBI, and other elements of the intelligence community and federal law enforcement.[12] Indeed, Congress designated CISA within DHS as the "lead cybersecurity and critical infrastructure" agency.[13] Congress explicitly gave CISA responsibility to develop and coordinate cybersecurity protocols across the government and to coordinate with the private sector.[14] Recent legislation also highlighted concerns around public disclosure of cyber incidents by exempting reports to CISA from the Freedom of Information Act.[15] That Congress has been so active with respect to cybersecurity, repeatedly bestowing authority upon executive branch departments and agencies but never to the Commission expressly,

---

[10] *NFIB v. OSHA*, 142 S. Ct. 661, 665 (2022).

[11] *See, e.g.*, Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022) § 2242(b)(1) (directing the CISA to promulgate regulations to implement the Act's reporting obligations for covered entities); Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C. § 652 (creating the CISA); Cybersecurity Act of 2015, 6 U.S.C. § 1504(a)(4) (directing the Attorney General and the Secretary of the DHS to develop guidance to promote sharing of cyber threat indicators with Federal entities); Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551, 3554 (codifying information security requirements for the federal government to be administered by the Office of Management and Budget and the DHS). Congress also annually enacts cybersecurity measures through the appropriations process. For example, this year, Congress expanded the CISA's budget by more than 28 percent, which was more than $460 million over the administration's request for the fiscal year. See Consolidated Appropriations Act, 2022, H.R. 2471, 117th Cong. (2022).

[12] *See* Cybersecurity Act of 2015, 6 U.S.C. § 1504(a)(4) (encouraging public and private sector entities to share cyber threat information with the federal government).

[13] 6 U.S.C. § 652.

[14] *Id.*

[15] *See* Consolidated Appropriations Act, 2022, H.R. 2471, 117th Cong. (2022).

speaks volumes about the Commission's lack of authority to enact the reticulated, prescriptive, mandatory rules in the Proposal.

II. The Proposal Is Not in the Public Interest and Would Undermine Cybersecurity.

We believe that the Proposal, considering existing guidance from the Commission, would not further advance the public interest, would undermine cybersecurity, and would impose substantial costs and burdens upon registrants with no corresponding benefit.

A. There Is No Need for the Commission to Further Address Cybersecurity Practice Through This Rulemaking.

The Commission has not explained why the Proposal is needed or required for *all* registrants. A rule is arbitrary and capricious unless an agency "examines the relevant data and articulates a satisfactory explanation for its action including a rational connection between the facts found and the choice made."[16] Registrants currently may, and do, report material cybersecurity incidents through 10-K forms, 8-K forms, press releases, and through other means. The Proposal does not identify any material harm, misinformation, or negative impact to registrants or investors from the current practices. Instead, it notes there may have been some inconsistencies among reports, and that the Commission "believes" that investors would benefit from the proposed requirements.[17] That is insufficient. Indeed, as noted below, the Commission has not identified any quantifiable or qualitative benefits that are substantially supported with evidence cited in the Proposal that would result from the Proposal's requirements. The lack of examination of relevant data or a reasoned explanation of why the Proposal is needed would render any final version of the Proposal arbitrary and capricious.

Moreover, the Proposal is unnecessary because investors already receive relevant information regarding a cybersecurity breach's effect on the health of a registrant under the Commission's current guidance on cybersecurity disclosures. The Commission's 2018 Interpretive Release instructs companies to "timely" disclose information in periodic reports about material cybersecurity incidents.[18] This guidance affords companies discretion to ascertain the relevant and material facts to be disclosed and acknowledges

---

[16] *Susquehanna Int'l Grp., LLP v. SEC*, 866 F.3d 442, 445 (D.C. Cir. 2017) (cleaned up).

[17] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590, 16,594 (proposed March 23, 2022) (to be codified at 17 C.F.R. pts. 229, 232, 239, 240, 249)..

[18] SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 1, 12 (Feb. 26, 2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

that "some material facts may not be available at the time of the initial disclosure," that a company "may require time to discern the implications of a cybersecurity incident," and that an "ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident."[19] The guidance ensures that investors receive information about material incidents without the attendant risks and unnecessary costs to registrants that the Proposal would impose. Although the Commission "observed certain cybersecurity incidents that were reported in the media but that were not disclosed in a registrant's filings" while registrants were operating under this guidance, the Commission does not fully explain why the 2018 guidance, when followed by registrants, is insufficient.[20] It in fact acknowledges that it is "unable to determine the number of material cybersecurity incidents that are not being disclosed in a timely manner."[21] Simply because the Commission observed a handful of instances in which cybersecurity incidents were not disclosed in accordance with the guidance does not mean that the guidance is insufficient. In our experience, the guidance is sufficient to inform investors about the financial health of a registrant. The Commission's objectives would be better met through further education surrounding the already issued guidance than by changing the regulatory requirements.

B. The Proposal Will Undermine Cybersecurity.

1. The Proposal's four-day timeline is too short for a public disclosure and will put companies at risk of further exploitation. Forcing registrants to report on this timeline, while incidents are still ongoing, publicizes that the company has at least one exploitable vulnerability to every bad actor throughout the globe, prompting them to search and potentially exploit a registrant's previously unknown access to their systems or data. This is wildly dangerous to any individual whose personally identifiable information may have been exposed and a specific reporting period may not give the registrant enough time to help protect vulnerable individuals. Again, forcing registrants to disclose even when the incident is ongoing alerts bad actors that the company is still vulnerable and leaves them susceptible to more attacks or breaches.

Although other regulations and laws require disclosure of a cyber incident within a shorter timeframe, there are safeguards against sharing that information and against disclosure to the public. For example, Congress recently passed cybersecurity reporting

[19] *Id.*

[20] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. at 16,594.

[21] *Id.*

legislation, discussed in more detail below, that requires companies to report cybersecurity incidents within 72 hours. But Congress included several liability protections that encourages timely reporting and protects companies who comply with the mandatory and voluntary disclosure obligations under the Act.[22] Similarly, some state security breach reporting laws require disclosure of a cybersecurity breach in less than four days, but these laws typically require disclosures to be made directly to affected persons and entities, rather than to the general public and also have other safeguards in place that delay a company's disclosure obligations.[23] A four-day period to publicly disclose a cyber incident may not allow a registrant enough time to fully realize the impacts of the incident or to fully remedy the exploited vulnerability before disclosing.

In addition to putting registrants at risk for further exploitation, the Proposal's timeline will divert a registrant's vital resources away from mitigating a cybersecurity incident and toward complying with reporting obligations. In the hours and days following a cybersecurity breach, companies must quickly and efficiently contain, minimize, and remedy any damage or loss resulting from the breach. Each of these measures must happen as soon as possible after a breach occurs and with the full attention of the registrant's resources and management—especially those devoted to cybersecurity. The Proposal's requirement to publicly report the incident while these actions are ongoing will disrupt these crucial response measures.

Moreover, the short timeline for public reporting will force companies to make consequential decisions about incident containment and remediation in a rushed and potentially higher-risk manner. Once a public disclosure has been made, cybersecurity personnel's options for containing a breach or attack while fully investigating the methods involved to improve security and prevent future attacks become limited. The inflexible four-day timeframe prioritizes speed of disclosure over safety and protection of information and critical resources.

2. Companies within the industry have complex supply chains and rely on different third-party service providers for capital projects and in support of industry operations. The complexity of these supply chains present inherent difficulties for companies to impose in-depth oversight for cybersecurity vulnerabilities. In addition, forcing

[22] *See* Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022).

[23] *See, e.g.*, O.C.G.A. 10-1-912 (Georgia's security breach notification law requires companies to notify relevant data owners if personal information was, or is reasonably believed to have been, acquired by an unauthorized person, within 24 hours of discovering a breach. The required notification may be delayed for law enforcement purposes). Each state has some version of a security-breach notification law.

disclosure of details regarding a company's vendor and supply chain information is likely to expose a registrant to further attacks. Cybercriminals have in the past exploited third-party vendors and software updates to infiltrate their customers' cyber infrastructure.[24] Any benefit from revealing the proposed information regarding third-party service providers would be outweighed by the increased risk of revealing potential targets.

3. Although the Proposal claims that what constitutes "materiality" for purposes of the proposed incident disclosures would be consistent with traditional definitions, the Proposal in effect suggests that the Commission anticipates some other metric of materiality than what is currently required to be disclosed within form 8-K. For example, the Proposal would require that issuers report "when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate."[25] This would require companies to categorize previously immaterial incidents as material, which goes against the definition of material. It is also difficult, cumbersome, and not useful for companies to report on prior incidents that did not raise to the level of material at the time, which is the entire point of the Commission proposal—to report on material cyber incidents.

Further, the Proposal asked for comment on whether to require reporting prior to a materiality designation. Many cyber events start by a simple phishing technique, and most events are easily contained and lead to no significant issue. Therefore, requiring registrants to report prior to determining whether an event is material would require registrants to potentially report on thousands, if not hundreds of thousands, of cyber-attacks that present no real threat to the financial health of the registrant. Notification of small events, prior to becoming material, would not benefit investors or prospective investors. To the contrary, it would confuse investors and lead to less-informed investment decisions.

4. Separately, the Proposal's guidance pertaining to what constitutes a "cybersecurity incident" is far too broad. Although the actual definition of "cybersecurity incident" is generally in line with established definitions of the term, the Proposal's guidance after this definition suggests broader application. For instance, the Proposal says that the term includes "a deliberate action or activity to gain unauthorized access to systems or to steal

[24] *See, e.g.*, Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (April 16, 2021), https://tinyurl.com/3bh4afr8.

[25] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. at 16,620.

or alter data."[26] This does not consider whether the company's security controls were sufficient to *prevent* a compromise of confidentiality, integrity, or availability of the system. If this example constitutes a "cybersecurity incident," the Proposal, if finalized, would result in excessive over-notification that would dilute the ability of an investor to determine cyber risk and would "hardly [be] conducive to [an investor's] informed decision making."[27]

We believe that adhering to traditional notions of materiality would continue to treat cyber incident reporting like any other event that would need to be disclosed within form 8-K. Registrants typically have a process to determine their own events that are material, and there is no need for special rules for resetting of what is considered material for reporting cybersecurity incidents.

5. The Proposal would effectively impose prescriptive one-sized-fits-all mandates with respect to board-member expertise with cybersecurity issues. To be sure, board members must be aware of cybersecurity threats to the company like they do for other important risks. For example, directors should understand company cybersecurity vulnerabilities and should be able to drive decisions regarding a company's overall efforts to guard against and address those risks. However, it is not clear why specific director expertise on cyber issues is necessary or relevant for all issuers and there should not be an expectation that most companies maintain a board of directors that has such an expert in cybersecurity—or that a company should have to explain why it doesn't have an expert on its board.

Board members do not need expertise in reverse engineering malware, the tactics, techniques, and procedures of foreign intelligence services and cybercriminals, or other highly technical computer-network operation topics. Instead, most registrants, and especially all large ones, will have a Chief Information Security Officer and significant access to technical expertise that can inform the board on addressing these issues and situations. In addition, the Proposal does not adequately describe how to even measure cybersecurity expertise among the Board or why having board members with technical expertise regarding cyber risks would be more beneficial than having other cybersecurity resources within a company. For example, individual technical degrees may not include the practical knowledge of leading teams that address current cybersecurity threats and incidents. Accordingly, the benefit case for needing cybersecurity-specific expertise on

[26] *Id.* at 16,601.

[27] *TSC Indus.*, 426 U.S. at 449.

the Board, or requiring an explanation of why not, does not appear to be clearly articulated by the Proposal.

III. The Commission Should Consider Several Amendments to the Proposal.

As previously noted, we do not believe that any change to the current disclosure requirements is necessary or appropriate as the status quo aptly serves registrants and investors. If the Commission does decide to move forward with some form of the Proposal, then it should amend the final version in several ways.

A. Elimination of Prescriptive Reporting Timeline

We believe that the four-day timeline for reporting of material cyber incidents is overly restrictive for the breadth of potential responses and registrants' actions to address exposed vulnerabilities. Therefore, if reporting cybersecurity breaches is required by the SEC at all, it should only be required within a reasonable time after the incident has been resolved.

B. The Commission Should Establish a Law Enforcement Exemption.

The broad disclosure of cybersecurity incidents, procedures, and prevention methods would pose threats to national security. The FBI and DHS, along with other elements of the intelligence community and federal law enforcement, should be able to request that companies withhold the disclosure of cybersecurity incidents during intelligence collection or a pending law enforcement investigation. As with all intelligence collection and investigations, publicly discussing or disclosing information about the matter significantly hinders the operation or investigation. As noted, most similar state disclosure laws provide such exemptions. Ultimately, aiding law enforcement in containing a cyber-attack and punishing wrongdoers best protects registrants, other companies, and investors.

For these reasons, any final rule should allow registrants to delay reporting of a cybersecurity incident whenever they are requested to do so by a state or federal law enforcement agency responsible for investigating cybersecurity incidents. The suggestion in the Proposal's request for comments that such requests come from the Attorney General is too narrow and would call for too much involvement from a cabinet-level official.[28] Rather, the Commission should grant such requests whenever requested by cybersecurity officials in the FBI, DHS or CISA, or state agencies responsible for

[28] *See id.* at 16,598.

investigating cybersecurity incidents who have received delegated authority to make such requests by the heads of those law enforcement agencies.

C. The Commission Should Establish a Critical Infrastructure Exemption.

Similarly, the Commission should consider an exemption from required disclosure for registrants within the critical infrastructure sector. The United States has identified 16 critical infrastructure sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[29] The vital nature of this infrastructure makes them a particularly attractive target to cybercriminals and other bad actors. That threat is so significant that the federal government created CISA specifically to work with the private sector to help protect critical infrastructure. The information required under the Proposal, as written, could include sensitive information that would undermine the security of critical infrastructure. Registrants that own, operate, or work with critical infrastructure should be exempted from any final requirements of the Proposal.

D. The Commission Should Provide Robust Liability Protections to Facilitate any Public Disclosure.

Any cybersecurity incident reporting structure should protect registrant information, include exemptions for reporting on personal data that has been compromised, and contain robust liability protections. For instance, Congress passed cybersecurity reporting legislation this year that includes needed liability protection for companies when disclosing cybersecurity incidents. Under the Cyber Incident Reporting for Critical Infrastructure Act, companies involved in particular infrastructure sectors must report certain cyber incidents to CISA within 72 hours and certain ransomware payments within 24 hours.[30] Because Congress recognized the concerns related to disclosing sensitive information in these reports, Congress protected reporting entities from certain liability associated with the submission of required or voluntary reports.[31] Under the Act, the incident reports and material used to prepare the reports cannot be received as evidence,

---

[29] *See* The White House, *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience (Feb. 12, 2013),* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[30] *See* Consolidated Appropriations Act, 2022, H.R. 2471, 117th Cong. (2022). These reporting obligations will not take effect until the Director of CISA promulgates implementing regulations. § 2242(b)(1).

[31] *Id.* §§ 2242(a)(1)(A), (a)(2)(A).

subject to discovery, or used in any proceeding in federal or state court or before a regulatory body.[32] Further, submitted reports must: (1) not be used by CISA, other federal agencies, or any state or local government to regulate, including through enforcement action, the activities of the entity that submitted the incident report; (2) be considered commercial, financial, and propriety information if so designated; (3) be exempt from disclosure under the Freedom of Information Act and similar disclosure laws; (4) not constitute a waiver of any applicable privilege or protection provided by law; and (5) not be subject to a federal rule or judicial doctrine regarding *ex parte* communications.[33]

In addition to demonstrating that Congress should lead on cybersecurity disclosure obligations rather than the Commission, this legislation demonstrates that liability protection for companies is paramount in establishing a working cybersecurity disclosure system. The Proposal, at the very least, should include the protections for registrants that the Cyber Incident Reporting for Critical Infrastructure Act includes for disclosing entities.

E. At Most, High-level Frameworks Rather than Specific Company Policies Should Be Subject to Public Disclosure.

Listing all cyber policies, procedures, governance structures, and management roles could result in exposing specific areas in which a registrant is vulnerable and provide intelligence to foreign nations, criminal enterprises, and other bad actors. The level of detail in the Proposal's required disclosures is not only dangerous, but it would also be more costly and simply unnecessary to inform investors about the risks that cybersecurity poses to the financial health of their investment.

Accordingly, any required disclosure should be at a high-level. Informing investors that a registrant has procedures, plans, and resources in place to prevent and respond to cyberattacks is sufficient for investors to make informed financial decisions. Descriptions of particular incidents should be limited to the general nature of the incident, its material impacts, and a high-level description of the measures in place to prevent reoccurrence. After all, these disclosures are designed for consumption by investors or prospective investors. The other detailed elements in the Proposal's required disclosures are not necessary and would not be an actual benefit to investors in making investment decisions. One alternative that would serve this purpose well is for registrants to disclose that they are complying with carefully curated cybersecurity safety frameworks. For instance, as

[32] *Id.* § 2245(c)(3).

[33] *Id.* § 2245(a)–(c).

mentioned previously, many registrants make their cybersecurity policies and procedures consistent with federal frameworks or standards, such as the NIST's Framework for Improving Critical Infrastructure Cybersecurity, which allows registrants to "apply the principles and best practices of risk management to improv[e] security and resilience."[34] Informing investors that a registrant is complying with these higher-level frameworks and standards would give them the comfort of knowing the company has policies, procedures, and processes in place to withstand a cyber-attack but with the benefit of not jeopardizing security in the process.

* * * * *

For the above reasons, API, AOPL and AFPM respectfully request that the Commission withdraw the Proposal and either retain the current reporting scheme or alter the Proposal substantially to establish several exemptions and to require only the disclosure of higher-level information regarding a registrant's cybersecurity frameworks.

We would be pleased to discuss these concerns further with you.

Sincerely yours,

Stephen Comstock, API - VP Corporate Policy

Andrew J. Black, AOPL – President and CEO

Jeff Gunnulfsen, AFPM – Senior Director

[34] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, (April 16, 2018), at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (While designed for companies involved in critical infrastructure, the framework "can be used by organizations in any sector or community.").