May 9, 2022

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

RE: File No. S7-09-22; RIN 3235-AM89: SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Dear Ms. Countryman,

The Energy Infrastructure Council ("EIC") is a non-profit trade association of companies that develop and operate energy infrastructure, including traditional and renewable energy infrastructure companies; investors in energy infrastructure; service providers; and other businesses and individuals that operate in and around the energy industry. The EIC appreciates the opportunity to respond to the U.S. Securities and Exchange Commission's ("Commission" or "SEC") request for public comment on the Commission's proposed rule, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" with respect to public companies subject to the reporting requirements of the Securities Exchange Act of 1934 (the "Proposal").[1] EIC writes today to provide the Commission with information regarding the work already being undertaken by EIC and our members to develop effective cybersecurity protections, as well as various comments and recommendations related to the Proposal.

I. EIC Members' Cybersecurity Efforts and Existing Regulations: The SEC Should Defer to the Primary Regulators of Critical Infrastructure Entities

a. EIC Members' Efforts and Existing Regulations

EIC and our members recognize the undisputed importance of cybersecurity to our country and economy, and to all public companies and their investors. While the Commission has a role to play with respect to Cybersecurity, we suggest the Commission proceed with caution and refer to existing rules, guidance, regulators, cybersecurity agencies and consumer protection authorities. Given the importance of critical infrastructure cybersecurity, we recommend the Commission consider the practices and procedures already implemented by cybersecurity regulators.

[1] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11038; 34-94382; RIN 3235-AM89 (proposed Mar. 9, 2022) (the "Proposal").

Our members have been implementing cybersecurity best practices for years. Many of our members are not only meeting current SEC best practices and guidance, but proactively addressing cybersecurity and investing in extensive cybersecurity protection. EIC and our members are already subject to multiple cybersecurity regulations, and the Proposal may add an administrative burden to our members while providing limited benefit to investors or the registrant.

EIC's members are subject to numerous regulations and directives related to cybersecurity. Two agencies within the Department of Homeland Security (DHS) have primary responsibility for pipeline cybersecurity: the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure Security Agency (CISA).[2] Other federal entities are also engaged with pipeline security, including the Department of Transportation's Pipeline and Hazardous Materials Safety Administration, which is the nation's pipeline safety regulator that partners with TSA on security issues, and the Department of Energy's (DOE) Cybersecurity, Energy Security, and Emergency Response office, which is congressionally mandated to research cybersecurity risks and coordinate federal response to energy sector cyber incidents.[3]

Extensive existing and upcoming regulations already guide EIC's members in cybersecurity. CISA has promulgated the Chemical Facility Anti-Terrorism Standards that require all high-risk chemical and industrial facilities, including oil and gas facilities, to comply with certain regulatory requirements.[4] These standards include completing security vulnerability assessments, developing site security plans, and implementing protective measures necessary to meet CISA-defined, risk-based performance standards.[5] In 2021, the TSA initiated a series of Security Directives for the nation's most critical pipeline systems, many of which are EIC members. These TSA guidelines include requirements that critical pipeline owners report security incidents to the TSA within 12 hours, comply with mandatory reporting measures, designate a cybersecurity coordinator, provide vulnerability assessments, and ensure compliance with certain cybersecurity requirements.[6] Additionally, TSA's current security guidelines include dedicated cybersecurity provisions which state that pipeline operators "should consider the approach outlined" in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, other guidance issued by DHS and DOE, and "industry-specific or other established methodologies, standards, and best practices."[7]

President Biden signed an Executive Order on May 12, 2021, on Improving the Nation's Cybersecurity, which primarily focused on improving federal agencies' cybersecurity defenses,

---

[2] *See* Chris Jaikaran, *Pipeline Cybersecurity: Federal Programs*, Congressional Research R46903 (Sept. 9, 2021), *available at* https://sgp.fas.org/crs/homesec/R46903.pdf.
[3] *See id.*
[4] *See Chemical Facility Anti-Terrorism Standards*, CISA, *available at* https://www.cisa.gov/chemical-facility-anti-terrorism-standards.
[5] *See id.*
[6] *See* Ratification of Security Directive Pipeline-2021-01, 86 FR 38209 (July 20, 2021); Ratification of Security Directive Pipeline-2021-02, 86 FR 52953 (Sept. 24, 2021).
[7] *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 16, 2018; *see also* Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Cybersecurity Capability Maturity Model (C2M2) Program, *available at* https://www.energy.gov/ceser/energysecurity/cybersecurity-capability-maturity-model-c2m2-program.

as well as improving the cybersecurity of the supply chain.[8] Then, on July 28, 2021, President Biden released a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, which directs CISA and NIST to develop and issue performance goals for critical infrastructure owners concerning cybersecurity.[9] This memorandum details U.S. policy to safeguard our critical infrastructure, with a particular focus on the cybersecurity and resilience of sectors and systems supporting the functions of government and the private sector so vital that their disruption would have a debilitating effect on our national or economic security or the public health and safety of the American people. The natural gas pipeline sector is one such system.

In furtherance of the President's focus to improve the safeguards of our critical infrastructure, the Industrial Control Systems Cybersecurity Initiative ("Initiative") was established. The Initiative is a voluntary, collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of technologies and systems that provide visibility, indicators, detections, and warnings of cyber threats that could degrade critical operations. The Initiative also encourages the sharing of threat information with the government to facilitate collective defense.

To coordinate natural gas pipeline sector input and effort, the Pipeline Subsector Coordinating Council (PSCC) formed a Natural Gas Pipeline CEO Task Force ("Task Force") to work with the federal government in developing and implementing the sector action plan. The Initiative effort for natural gas pipelines began on August 31, 2021. In support of this effort, the Task Force met biweekly with the participation of senior government officials from the National Security Council, the Office of the National Cyber Director, the Transportation Security Administration, the Department of Transportation/PHMSA, Cybersecurity and Infrastructure Security Agency, and the Department of Energy. Private sector participation included CEO representation from some of the key companies in the industry. To date, most priority pipelines have deployed or committed to deploy additional cybersecurity technologies.

Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act, which will require critical infrastructure entities to report material cybersecurity incidents and ransomware payments to CISA within 72 and 24 hours, respectively.[10] CISA must promulgate a proposed implementing regulation within 24 months from the final enactment date of March 15, 2022, and a final regulation no later than 18 months thereafter. The Act also calls for harmonization of cybersecurity reporting that would help avoid counter-productive and burdensome conflicts and redundancy.

---

[8] Executive Office of the President, *Improving Nation's Cybersecurity*, 86 FR 26633 (May 17, 2021).
[9] The White House, *Improving Cybersecurity for Critical Infrastructure Control Systems*, NATIONAL SECURITY MEMORANDUM (July 28, 2021), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/nationalsecurity-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.
[10] Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022). As drafted, the reporting requirements will cover multiple sectors of the economy, including chemical industry entities, commercial facilities, communications sector entities, critical manufacturing, dams, financial services entities, food and agriculture sector entities, healthcare entities, information technology, energy, and transportation.

The Proposal justified its overly broad approach to materiality on presumption (without substantiation) that there is currently systematic under-reporting of material cybersecurity incidents to investors, stating that "certain cybersecurity incidents were reported in the media but not disclosed in a registrant's filings."[11] However, public companies are already under an obligation to report to investors any material incidents. In 2018, the SEC published a Release titled "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," which emphasized a range of factors that may affect whether an incident should be disclosed to investors beyond the bottom-line financial costs to respond to the incident.[12] There is no record of public companies – critical infrastructure or otherwise – systematically or regularly failing to provide timely material information to investors about material cybersecurity incidents. The fact that some incidents are reported in the press is not necessarily indicative of their materiality.

b. Recommendations

EIC recommends that the Commission consider and defer to those entities with primary responsibility over cybersecurity, especially for critical infrastructure entities such as many of EIC's members. The Commission should consider an express exemption for reporting by critical infrastructure entities that are actively engaged in addressing an incident with their primary regulators and cybersecurity agencies. The Commission should also rely on existing requirements for public companies to report material events and maintain internal controls as set forth in the Commission's 2018 statement and guidance on public company cybersecurity disclosures[13] and 2018 report of investigation concerning cyber-related internal accounting controls.[14] In the event the Commission proceeds with the Proposal, it should refine its guidance to provide more clear direction about material incidents, and ensure it does not counterproductively induce harmful overreporting (discussed further below).

II. Incident Reporting Requirements: The Commission Should Reconsider Its Four-day Reporting Deadline and Level of Specificity Required for Material Cybersecurity Disclosures

a. The Definition of Materiality Is Not Clear Due to the Provided Examples of Potentially Material Cybersecurity Incidents, and Could Lead to Over-Reporting of Cybersecurity Incidents

The proposed materiality standard is not clear, and it fails to provide sufficient additional guidance on how to make this determination for cybersecurity incidents. The Proposal lacks concrete thresholds to assist registrants in determining materiality. Specifically, many of the examples of material cybersecurity incidents in the Proposal would not constitute a material

---

[11] The Proposal at 52.

[12] *See Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 17 CFR Parts 229 and 249, SECURITIES AND EXCHANGE COMMISSION (Feb. 21, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[13] *Id.*

[14] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, Securities Exchange Act of 1934 Release No. 84429 (Oct. 16, 2018), *available at* https://www.sec.gov/litigation/investreport/34-84429.pdf.

cybersecurity incident if managed through effective incident response, remediation and resiliency. Additionally, it is rare that a cybersecurity incident is immediately apparent as material.

While the Proposal does not purport to change the traditional materiality standard for reporting cybersecurity incidents, the SEC appears to be signaling (including by citing examples of some potentially routine types of incidents) that it expects registrants to err on the side of more reporting, and to do so particularly quickly. That is problematic because breaches and cyber events can be notoriously fluid, and a company's early understanding of an incident (and available remediation and resiliency measures) can change significantly (in both directions) during the course of a sophisticated forensic investigation. Moreover, any incident that is potentially material to a public company will very likely involve law enforcement and other government agencies besides the SEC, and various equities and interests will be implicated. Public disclosure of serious and complex incidents should therefore not be inappropriately rushed.

Furthermore, if registrants are incentivized to report what may be non-material incidents early to err on the side of caution, the result may be stock price drops as the market reacts to being informed of putatively material cybersecurity events. However, if in the fullness of time, the incident turns out not to have been material itself, the but-for cause of any impact on stock price would be the SEC-incentivized (over-)reporting.

b. Four-days Is a Rigid Timeline that May Not Be Sufficient Time to Fully Understand the Scope of an Incident

The Proposal provides some helpful guidelines and flexibility for reporting material cybersecurity incidents. However, requiring registrants to report material cybersecurity incidents four days after determining the incident is material may add an unnecessary burden for registrants, diverting resources to public disclosure of fluid facts in the middle of time-sensitive containment and mitigation activities.

For instance, during the first few days of a cybersecurity incident, a company will often initiate an incident response plan and collaborate with forensic experts to: determine the possible attack vectors and any indicators of compromise; gather and review evidence such as system events, logs of affected systems, and other pertinent information; notify any relevant stakeholders and/or fiduciary obligations; contain an ongoing incident such as through isolating compromised networks or systems, closing vulnerable ports and access points, or re-routing or filtering network traffic; eradicate a threat such as by removing malware, disabling breached user accounts, or patching vulnerabilities; and monitor for any additional anomalous activity, signs of intrusion, or indicators of compromise.

During an incident investigation, a registrant's understanding of the incident naturally evolves. Disclosing an incident quickly could cause inadequate reports to be filed, which should not yet be relied upon, and which could lead to media and other questions that distract from core incident response and remediation efforts, as well as investor confusion. Moreover, publicly disclosing information that law enforcement, national security agencies, or regulators could utilize in an investigation could impede the proper course of the investigation and cause

unintended consequences, such as revealing sensitive information upon which bad actors might act. Other regulators with strict reporting deadlines do not publicly disclose information related to ongoing investigations. Indeed, other regulators that request information on security incidents, such as CISA and the FBI, have stressed that their agencies do not share breach report data with regulatory agencies such as the FTC or SEC.[15] The TSA directives related to cybersecurity treat information concerning security incidents as Sensitive Security Information, which is exempt from public disclosure.[16]

Additionally, the complexity of critical infrastructure incidents often involves extensive interaction, coordination and joint remediation with government regulatory, cybersecurity, law enforcement and homeland/national security agencies, as well as upstream and downstream partners. Requiring disclosure within four days of determining presumptive materiality would disrupt this complex process. Premature public reporting would be in conflict with the principle of "responsible disclosure"[17] and would risk potentially significant adverse consequences for companies, investors, the economy, and safe functioning of society's critical infrastructure. The SEC's four-day public disclosure proposal does not take this complex and essential balance into account.

Finally, the reporting requirements under the Proposal are also not aligned with other federal and state cybersecurity incident reporting requirements. Each registrant has a number of obligations under either federal or state law in the case of a security incident. Several states have security incident reporting rules, each with different variations of timing. Moreover, CISA is currently drafting implementing regulations for critical infrastructure entities after the passing of the Cyber Incident Reporting for Critical Infrastructure Act. The Proposal would add another compliance burden – with a significantly shorter period of time than most other regulations to report the incident to the public and Commission. The Commission should consider aligning its reporting obligations with other state and federal laws.

Most importantly, the SEC must not require public disclosure while a registrant is involved in complex event management with the government agencies responsible for protecting the nation's critical infrastructure where such agencies believe public disclosure would harm the national interest. The Commission must allow delayed public reporting in those circumstances. Additionally, we foresee threat actors using the knowledge of a company's reporting requirements during an active incident (such as ransomware) as leverage in negotiations with such a company.

---

[15] *See* Ben Kochman, *Biden Cyber Officials Pitch Partnership Amid Hacking Threat*, LAW360 (Apr. 22, 2022), *available at* https://www.law360.com/corporate/articles/1482974/biden-cyber-officials-pitch-partnership-amid-hacking-threat.

[16] *See* Chris Jaikaran, *Pipeline Cybersecurity: Federal Programs*, Congressional Research R46903 (Sept. 9, 2021), *available at* https://sgp.fas.org/crs/homesec/R46903.pdf; *see also* 49 C.F.R. §1520.

[17] Responsible disclosure entails holding off on public disclosure until the responsible parties have been allowed sufficient time to patch or remediate the vulnerability or issue. *See CISA Coordinated Vulnerability Disclosure Process,* CISA, *available at* https://www.cisa.gov/coordinated-vulnerability-disclosure-process.

c. Public Disclosures of Material Cybersecurity Incidents May Have Severe Security Implications

Under the Commission's current Proposal, registrants would be required to publicly disclose certain incidents that are still in the process of being investigated or remediated. The proposed real-time and after-the-fact reporting of cybersecurity incidents could also have the unintended consequence of providing critical information not to investors, but to threat actors in the middle of an attack. Such information could provide the threat actors with an advantage in creating persistence in the network, prolonging an attack, negotiating a ransom, or valuing stolen data on the dark web. Requiring disclosure prior to full remediation may signal to the current threat actor or other bad actors that the registrant continues to have a vulnerability that can be further exploited and may otherwise jeopardize internal remediation efforts. Disclosure prior to remediation may also make the registrant more susceptible to other attacks: while the registrant's resources are focused on remediating the disclosed issue, the malefactor or other bad actors may look to attack the registrant's environment more broadly in the hope of identifying other vulnerabilities to exploit. Additionally, it is not clear that requiring such detailed disclosures will provide either significant benefits or useful information to investors.

d. Form 8-K Should Not Be Expanded to Require Disclosure of Operational Developments in Real Time

Cybersecurity incidents are fundamentally different from the types of events covered by existing Form 8-K rules. Mandatory Form 8-K triggers generally cover discrete, clearly identifiable events relating to a company's material transactions, governance or financial position. The occurrence and timing of most 8-K triggers are typically either within the control of the company or reasonably predictable. As acknowledged by the Commission in 2004, reporting on 8-K is intended for "unquestionably or presumptively material events."[18]

Conversely, a cybersecurity attack is by its nature operational, largely outside the company's control and unpredictable, and certainly not "unquestionably or presumptively material." Additionally, a cybersecurity incident often takes multiple days or weeks to discover, assess and remediate. When an event is discovered, a company's attention and resources are better fully dedicated to assessing and remediating the event and shoring up protections of the company's systems, all of which are in the best interests of the company and its investors. Given the four-day timeline and potential strain on company resources, a company may err on over-reporting an incident that appears potentially material depending on what could be learned and the way the incident may unfold, which after a thorough investigation, is determined not material.

Existing rules already require companies to apprise investors of a material operational issue, including a material cybersecurity event. A specific, mandatory 8-K trigger for cybersecurity events inappropriately extends the coverage of Form 8-K to the realm of

[18] 17 C.F.R § 228, 229, 230, 239, 240 and 249 (2004). ("Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date").

operational developments, which are more appropriately disclosed in periodic reports or voluntary Forms 8-K, at a point when the information is more fully developed and impacts are better understood. As discussed in the SEC's 2018 guidance, Form 10-K, Form 10-Q and Securities Act prospectus requirements call for disclosure about the material impact of a cybersecurity event, and companies should use Form 8-K to reduce the risk of selective disclosure and the risk of trading on the basis of material nonpublic information.[19]

III. Board and Governance Requirements Create Undue Administrative Burdens

The Proposal's Item 106 of Regulation S-K and Item 16J of Form 20-F include requirements for registrants to disclose information such as: the cybersecurity expertise of its board members; the registrant's cybersecurity policies and procedures; whether it employs a chief information security officer; and the interactions of management and the board of directors concerning cybersecurity. This will create an administrative burden and lead to registrants designing policies and procedures for purposes of SEC reporting rather than broader compliance goals based on risks specific to an organization.

Additionally, requiring the disclosure of cybersecurity expertise for a member of the board of directors may be difficult while providing limited benefit to investors. Boards of directors are distinct from management, as the board's role is one of oversight whereas management is required to have subject matter expertise. The board should have the flexibility to determine its own composition, and needs, and take into consideration the collective expertise of the board, holistically. Boards are, by design, deliberative bodies and tasked with oversight of numerous risks – of which cyber is only one of those risks. Current disclosures required concerning board's business experience should be sufficient to elicit relevant information for investors.

IV. Cybersecurity Disclosure Requirements Will Provide a Roadmap for Bad Actors

The Proposal may inadvertently lead to cybersecurity incidents. The Proposal will likely lead to registrants disclosing granular and specific details about cybersecurity incidents as well as overly detailed information regarding their cybersecurity governance. Accordingly, the Proposal may provide threat actors with a "roadmap" to potential vulnerabilities in registrant's cyber controls and associate information systems. Prior to engaging with a target, threat actors will often use open-source intelligence (OSINT) to learn more about their target.[20] We can foresee threat actors using SEC disclosures to target registrants they perceive to have unsophisticated cybersecurity programs. For instance, a threat actor may target a registrant that disclosed that it is in the process of implementing cybersecurity policies and procedures, or a registrant that disclosed that its chief information security officer unexpectedly quit, and the position is currently vacant. Additionally, threat actors may target cybersecurity-related personnel that are named in a registrant's disclosures. Providing such a roadmap to threat actors

[19] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 17 CFR Parts 229 and 249, SECURITIES AND EXCHANGE COMMISSION (Feb. 21, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.
[20] *See Open Source Intelligence (OSINT)*, CROWDSTRIKE (Feb. 25, 2022), *available at* https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/.

could be particularly problematic for critical infrastructure companies, where such a roadmap could have major economic and national security implications.

V. The Commission Should Consider the Costs of Compliance for the Regulation

The Proposal will result in the inevitable duplication with the regulation and responsibilities of more appropriately relevant agencies. EIC members have already substantially invested in cybersecurity compliance and best practices. For example, many EIC members have already invested substantially in complying with existing Pipeline regulations, including the TSA's directives from 2021. This resulting burden and complexity distract cybersecurity professionals from identifying and protecting against the threat environment, while bringing limited benefits to investors as well as to EIC members' cybersecurity programs, and providing substantial compliance costs to registrants.

VI. Specific Responses to Requests for Comment (RFI)

a. RFI 1: We encourage the Commission to reconsider the four-day reporting period, as several circumstances may warrant holding off from public disclosure, and the burdens on registrants will vary depending on materiality and any requirements that law enforcement may impose on releasing information. Specifically, we recommend material cybersecurity incidents be reported as an initial, brief update (assuming approval from law enforcement or relevant cybersecurity or national security agencies), followed by an updated 8-K or 10-Q at a later date.

b. RFI 2:

i. We recommend the Commission revise the incident reporting form to include only a general description of an incident's high-level details, such as the basic nature, scope and impact of the incident. Proposed Item 1.05 should only cover the basic impact at a high level, and it may be more beneficial to release an initial 8-K with limited information and, if necessary, follow up at a later date with an updated 8-K to the extent important information becomes available or needs to be corrected.

ii. Greater clarity would be helpful for the relevant parameters of materiality in the cybersecurity context. Registrants should be permitted to make their own determination of incidents that rise to the level of notification—and these considerations should include ensuring that any publicly disclosed information does not put the registrant at further risk, and does not confuse investors about the actual investment-related significance of an incident.

c. RFI 3: Proposed Item 1.05 may have the unintentional effect of putting registrants at additional risk. Accordingly, the Commission should limit the information required by proposed Item 1.05 to only cover the basic impact at a high level.

d. **RFI 4:** The four-day timeline is not enough time to provide a detailed level of information for public disclosure and the Commission should consider modifying the timeframe to an initial, brief update (assuming approval from law enforcement or cybersecurity or national security agencies) followed by an updated 8-K or 10-Q at a later date.

e. **RFI 5:** Yes, the Commission should consider a quantifiable threshold for materiality that would be similar to other financial losses for materiality determinations. We recommend the Commission clarify that a registrant's traditional assessments concerning materiality (including available mitigation), and analysis thereof, will continue to apply.

f. **RFI 6:** Proposed Form 8-K will create a conflict for some critical infrastructure companies with respect to the TSA as well as the upcoming CISA regulations under the Cyber Incident Reporting for Critical Infrastructure Act.

g. **RFI 7:** Yes, the Commission should allow registrants to delay reporting where the Attorney General (and other prudential cybersecurity regulators) has requested such a delay.

h. **RFI 8:** Yes, the Commission should provide further guidance regarding the timing of a materiality determination and should include time for registrants to conduct incident response and forensic investigations. The Commission should also consider exemptions for critical infrastructure entities and companies that are collaborating with law enforcement, or other cybersecurity or national security agencies.

i. **RFI 10:** No, registrants would not always be reasonably able to obtain information to make a materiality determination concerning cybersecurity incidents. Recent examples of this include SolarWinds, Okta, Log4j, and Microsoft Exchange Server, where registrants may have been dependent on third parties to confirm whether they were impacted. The Commission should consider exceptions for such dependencies.

j. **RFI 16:** Further clarification is needed on the time period for when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate. How far back would registrants be expected to go?

k. **RFI 18:** Yes, "operational technology" would be helpful to define.

l. **RFI 19:** "Cybersecurity" should be defined and should be aligned with the NIST-CSF (identify, protect, detect, respond, recover).

m. **RFI 20:** It should be optional for registrants to specify whether any cybersecurity assessor, consultant, auditor, or other service that it relies on is through an internal

function or through an external third-party service provider. However, registrants should not be required to mention company names or vendors used.

n. **RFI 21:** Registrants should not have to explicitly state that they do not have any established cybersecurity policies and procedures or other comprehensive details concerning companies' cybersecurity governance.

o. **RFI 22:** There are concerns that certain disclosures required under Item 106 would have the potential effect of undermining a registrant's cybersecurity defense efforts or have other potentially adverse effects by highlighting a registrant's lack of policies and procedures related to cybersecurity. Instead of being prescriptive, we recommend the Commission create a section for registrants to describe their cybersecurity protections as part of their overall risk management program. Many registrants already detail this in their annual report voluntarily.

p. **RFI 27, 29, 32, and 34:** Cybersecurity expertise should be approached the same way it is treated for other specialties, such as accountants, legal, operations, and other areas of expertise.

We thank the Commission for the opportunity to provide our thoughts, and respectfully request that the Commission take our recommendations into account when considering the Proposal. We would be happy to discuss our comments or any other matters that you believe would be helpful. Feel free to contact me at 202-747-6570 if you have questions or would like to discuss our comments.

Sincerely,

Lori E. L. Ziebart
President & CEO
Energy Infrastructure Council