Edison Electric
INSTITUTE

Via E-Mail (rule-comments@sec.gov)

May 9, 2022

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

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

Dear Secretary Countryman:

Thank you for the opportunity to provide comments on the proposed rules. We applaud the ongoing efforts of the Commission to enhance and standardize disclosures on cybersecurity risk management, strategy, governance, and incident reporting.

The Edison Electric Institute (EEI) is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for more than 220 million Americans and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. In addition to our U.S. members, EEI has more than 60 international electric companies as International Members, and hundreds of industry suppliers and related organizations as Associate Members. Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums. Our industry input is based on our extensive experience in addressing cybersecurity risks and attacks against the power grid.

EEI recognizes the hallmark principle of U.S. securities laws is transparency and that the statutes and rules are designed to provide investors with the disclosures that they need in order to make informed decisions. EEI and our members support several key elements of the cybersecurity reporting approach contemplated by the Commission's proposal. Cybersecurity is of the utmost importance to our investors and warrants a set of rules and guidelines that are cybersecurity-specific. However, it is imperative that the Commission implement rules that recognize the inherent sensitivity of and the need for protection of information regarding cybersecurity, including the risks associated with cybersecurity incident disclosure, and allow reasonable flexibility regarding the governance of cybersecurity within registrants.

Disclosure of cybersecurity information must properly balance the incremental benefits associated with broader disclosure against the known risks that may result from public disclosure.

National Security and Law Enforcement

Consideration should be given to national security and law enforcement. While broad disclosure of information on cybersecurity incidents may hold some value to investors, paradoxically it disproportionately benefits sophisticated adversaries and other malicious actors. Whether they are nation-state cyberterrorists or something less coordinated, malicious cybersecurity actors are constantly monitoring and scanning for vulnerabilities, weaknesses, potential attack vectors, and cyber targets. Public disclosure of a cyber incident, especially before the incident is mitigated, provides details on vulnerabilities and attack vectors that become a useful roadmap for malicious actors, which makes the registrant, and others, a target for ongoing or similar attacks. The proposed SEC rules must strike the proper balance between enhancing transparency of cyber incidents for investors, on the one hand, and avoiding disclosure of information that is not useful to investors or can facilitate malicious actor efforts to jeopardize national security or the efforts of law enforcement, and particularly the integrity and reliability of the electric grid.

Our industry is one of the sixteen critical infrastructure sectors identified by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). CISA further states that, "without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. Presidential Policy Directive 21 identifies the Energy Sector as uniquely critical because it provides an 'enabling function' across all critical infrastructure sectors."[1] As such, the safe and reliable operations of the electric grid is a primary consideration when analyzing the risks associated with disclosing potentially sensitive operational details. Given the critical nature of our members' operations, they also are likely to possess some of the nation's most critical confidential information, including cybersecurity threat information furnished by government entities, such as the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the National Security Agency (NSA). Many of the information-sharing agreements and requirements between our members and these entities preclude the sharing of certain information with any outside stakeholders, let alone publicly with investors. In these situations, registrants should not be liable for not filing an Item 1.05 Form 8-K or failing to make similar disclosures that could jeopardize national security interests.

There are additional considerations when individuals with security clearance who work for registrants receive sensitive information, such as by National Security Letter or notification of a breach through the Sector Specific Agency, which for our sector is the Department of Energy (DOE), or a law enforcement agency. These individuals would be forbidden under penalty of criminal law from disclosing this information. The conflict between criminal law and regulation must be addressed for disclosure requirements to be reasonable.

[1] U.S. Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/energy-sector).

Consideration also should be given to situations where related information may be considered less sensitive, although still confidential and subject to jurisdiction by a registrant's Sector Risk Management Agency (SRMA), which also is DOE for our industry. We suggest that our members be permitted the flexibility to work with such agencies to properly assess the risk associated with disclosure of potential information, and file delayed, redacted, or no disclosure, as appropriate.

The Sensitivity of Cybersecurity Information Favors a Balanced Approach to Disclosure

EEI members provide safe, affordable, reliable, and secure electric service to their customers. Electric companies have robust existing regulatory requirements pertaining to cybersecurity protection and incident reporting, including DOE requirements and the requirements developed by the North American Electric Reliability Corporation (NERC) and approved by the Federal Energy Regulatory Commission (FERC), which are also enforced by NERC and FERC.[2] Electric companies are committed to compliance with these and other standards. Violations of NERC requirements are subject to significant fines, and the focus of the incident reporting is compliance with NERC standards and protection of the bulk-power system, rather than review in public. Other federal agencies – particularly but not exclusively those charged with oversight of critical infrastructure – consistently have taken considerable measures to protect exposure of information about critical infrastructure that could be valuable to attackers. For example, NERC and FERC do not publicly disclose certain sensitive information regarding the security of the bulk-power system that could otherwise be available to bad actors.[3] Indeed, greater disclosure could create a forum for bad actors to aggregate and analyze data related to cyber system weaknesses in general or, when combined with other publicly available information, may help an attacker. Given the highly technical nature of the electric grid, its complex operations, and the sensitivity of the information that is required to maintain its security, public disclosure of cybersecurity information carries significant risks for the security and reliability of the electric grid.

The interest in transparency for investors must be balanced against the associated security and electric reliability risks that flow from public disclosure of sensitive cybersecurity information (*e.g.*, Critical Energy/Electric Infrastructure Information (CEII) and other regulated data), recognizing that disclosure of cybersecurity information creates additional risk that adversaries can use to better target their attacks on a specific registrant or to take advantage of trends or other

[2] *See, e.g.,* Reliability Standard (Critical Infrastructure Protection) CIP-008-6 — Cyber Security — Incident Reporting and Response Planning which requires electric companies to mitigate the risk to the reliable operation of the bulk electric system as the result of a "Cyber Security Incident" by specifying incident response requirements. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf.

[3] *See, generally,* FERC and NERC "Second Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards," September 23, 2020, available at https://www.ferc.gov/sites/default/files/2020-09/Second%20Joint%20White%20Paper_CIP%20NOP%20Confidentiality_09.23.2020_AD19_18_000_0.pdf

vulnerabilities.[4] FERC and DOE have established procedures for how they designate, protect, and share CEII.[5] Cybersecurity information is often highly technical, extremely sensitive, and requires specialized training and expertise to understand, reducing its value for investment decisions; however, attackers who do have the specialized knowledge, expertise, and malign intent may be able to use this information to target specific electric companies and the electric grid in general. Further, broad publication of this information before an incident or vulnerability has been mitigated encourages further attacks against the registrant or other targets that may share a similar vulnerability, which could result in disastrous consequences to the registrant, their customers, and their investors, as well as more broadly the electric subsector.

Information should not be required to be shared publicly if a registrant believes that there is a reasonable risk that the disclosure will expose it or others to ongoing or additional risks of cyber-attacks.

The SEC proposal requires registrants to disclose a significant amount of cybersecurity detail. For example, the SEC's proposed addition of Item 106(d)(2) would require a registrant to disclose when a "series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate." According to the SEC, registrants would be required to "analyze related cybersecurity incidents for materiality, both individually and in the aggregate." The SEC would require registrants to disclose the following elements if incidents become material in the aggregate:

1. When the incidents were discovered and whether they are ongoing.
2. A brief description of the nature and scope of such incidents.
3. Whether any data was stolen or altered.
4. The impact of such incidents on the registrant's operations and its actions.
5. Whether the registrant has remediated or is currently remediating the incidents.

While that level of information may potentially be useful to investors, it might be devastating to a registrant while a cyber attack is still underway. Diverting time and valuable resources to create a report while the registrant is trying to mitigate the incursion creates additional risk as the same resources are likely to be drawn on for both efforts. Additionally, the requirement to evaluate past incidents continually to determine whether the materiality threshold is met would further distract resources that should be focused on the more-immediate need of securing the system. Aside from publicly disclosing the registrant's awareness of the attack to the attacker, which may be undesirable or may be contrary to the requests of federal agencies such as the DHS or the FBI, doing so possibly invites other attacks.

[4] The Fixing America's Surface Transportation Act (FAST Act) added section 215A to the Federal Power Act, which authorizes both the Secretary of Energy and the FERC to designate information as CEII. 129 Stat. 1312. CEII is a category of controlled unclassified information about a system or asset of the bulk-power system, whether physical or virtual, that if destroyed or incapacitated, would negatively affect the United States' national security, economic security, public health or safety, or any combination of such effects.

[5] Critical Electric Infrastructure Information; New Administrative Procedures, 85 Fed. Reg. 14756 (2020).

There may be value in providing certain information to investors, but it should not come at the expense of ensuring a reliable and secure electric grid. Registrants should be allowed to weigh the benefits of sharing incremental information with the public against the potential national security or public safety consequences that would result from a cyber incident.

Proposal on Reporting of Cybersecurity Incidents

We recognize the importance of reporting material cybersecurity incidents to investors, and we generally support the proposal to require registrants to disclose material cybersecurity incidents in a current report on Form 8-K within four business days after a materiality determination is made, subject to the certain liability protections and exceptions we are suggesting the Commission adopt. However, given that all cybersecurity incidents are not created equally, the disclosure requirements need to be carefully limited to "material" information and to information that will not further the risks described above. Below are a few specific suggestions:

- We propose that a new Section 1.05(c) be added to Form 8-K that would read as follows:

  > (c) No disclosure under Item 1.05(a) shall be required to the extent that (i) such disclosure is prohibited by the rules of, an agreement with, or written instructions from an appropriate governmental authority, or (ii) the registrant in good faith concludes that its disclosure will expose it or others to ongoing or additional risks of a cybersecurity incident.

  Note that this limitation applies only "to the extent" that disclosure would trigger either clause (i) or (ii). As a consequence, some disclosure likely still would be required, but disclosure that would have an adverse impact would not be.

- We also propose that a new instruction to Item 1.05 be added that would read as follows:

  > 4. The appropriate governmental authorities referenced in Section 1.05(c) would include the agencies, commissions, departments and authorities of Federal or state governments with authority over the registrant, or its subsidiaries or affiliates, with respect to cybersecurity, the disclosure of cybersecurity incidents, and the enforcement of cybersecurity laws.

- We suggest that the SEC refine Item 106(d)(1)(ii) so that it covers only "any future impacts . . . that the registrant believes are reasonably likely to be material." Our concern is that the proposed standard uses the word "potential," which is all-encompassing and does not, on its face, exclude unlikely or low-probability outcomes.

- We suggest that the SEC refine Item 106(d)(1)(iii) to clarify that it requires disclosure of only "material" remediation. In the ordinary course it is typical to respond to major

cybersecurity incidents for an almost indefinite period, often in immaterial ways[6]. It should be clarified that immaterial remediation does not require disclosure, as such information is not valuable to investors.

- The new rules should permit registrants to defer follow-on disclosure until remediation is sufficiently complete such that disclosure would no longer increase the risk of further harm to security or reliability. Consistent with the language that we propose for Item 1.05(c) of Form 8-K, we suggest that a new paragraph be added to Item 106 that would read as follows:

  > (c) No disclosure under Item 1.05(a) shall be required to the extent that (i) such disclosure is prohibited by the rules of, an agreement with, or written instructions from an appropriate governmental authority, or (ii) the registrant in good faith concludes that its disclosure will expose it or others to ongoing or additional risks of a cybersecurity incident.

- We also propose that a new instruction to Item 106 be added that would read as follows:

  > The appropriate governmental authorities referenced in Section 106 would include the agencies, commissions, departments and authorities of Federal or state governments with authority over the registrant, or its subsidiaries or affiliates, with respect to cybersecurity, the disclosure of cybersecurity incidents and the enforcement of cybersecurity laws.

- For the reasons noted above, we suggest the SEC limit Item 106(d)(1)(iv) to "material changes."

- We suggest that the SEC limit Item 106(d)(2) disclosures to a "series of related and previously undisclosed" cybersecurity incidents and ones occurring within the two-year period prior to the filing[7]. Otherwise, the unspecified, and therefore open-ended, time period would require an unwarranted tracking effort and potentially produce reports on an aggregation of incidents over a lengthy period of time that likely have no current relevance to investors and that may not bear relation to each other.

- We also strongly urge that the final rule maintain the current proposed standard that untimely filing of an Item 1.05 Form 8-K Item does not affect Form S-3 eligibility.

[6] For example, a registrant may, following a Form 8-K report of a cybersecurity incident, among other actions, require more frequent password changes. Clearly that does not warrant coverage in a Form 10-Q or Form 10-K.
[7] Some registrants do not currently track incidents in a way that would enable their aggregation. Even a two-year requirement would need to be phased in.

Proposal Regarding the Board of Directors' Cybersecurity Expertise

Investors are increasingly asking for enhanced disclosure by registrants regarding oversight of cybersecurity. Specifically, we have heard calls from investors for a disclosure of a qualitative discussion of the role of the board of directors in establishing cybersecurity policy and in overseeing its implementation. We agree with the Commission that investors are interested in knowing that registrants and their boards are taking cybersecurity seriously and addressing the risks comprehensively. We believe, however, that disclosure about whether any members of the registrant's board of directors have cybersecurity experience or expertise is best located in proxy statements, where other corporate governance-related information currently is disclosed and where many issuers already discuss board cybersecurity oversight and expertise.

Proposal Regarding Management's Role and Expertise

We are concerned that the proposal focuses too much, either directly or by implication, on the granular components of a registrant's cybersecurity structure and the experience and expertise of management. Structures, in themselves, are not indicative of good processes, and company personnel will change over time, particularly within an IT structure, making some of the proposed disclosures potentially obsolete shortly after filing. Moreover, the detailed information called for is not information that is important to investors. We expressly asked a broad range of both buy-side and sell-side analysts covering electric and gas utilities what disclosure they would like to see, and their message has been consistent: **They do not want the granular details; rather, they want an overview that provides them assurance that appropriate attention is being paid to cybersecurity issues by management and the board**. As a result, we suggest that Item 106(c)(2) be simplified to read as follows:

> Describe generally the structure within management that oversees the registrant's cybersecurity policies, procedures, and strategies, including, if not disclosed elsewhere, the general processes through which cybersecurity incidents are identified, reported *among management, the board, regulators, and the public*, and remediated.

We also do not believe that the identification of individuals or their credentials is warranted. This disclosure could further subject registrants to social engineering campaigns[8] by specifically identifying their key players to bad actors. We suggest that the rules require a high-level description of cybersecurity oversight and monitoring rather than a detailed description or organizational chart.

[8] Social engineering campaigns orchestrated by outside actors use deception to manipulate key people into divulging confidential or personal information that may be used for fraudulent purposes. Social engineering campaigns utilize a variety of methods such as phishing (spear phishing, whaling, pharming, etc.) and vishing. Phishing attacks attempt to obtain personal or sensitive information through electronic communications and have become very sophisticated. The more information the outside actors have about a target entity's employees, the more likely the outside actors will be able to identify vulnerabilities and target them successfully.

Further Recommendations

Unnecessary Exposure to Liability

We believe the Commission may be underestimating the sophisticated analysis and subjective judgment required to determine whether a material cyber incident has occurred and to determine what disclosures may be required. Even determining that a cybersecurity incident has occurred (as contrasted with a simple IT failure) may depend on a forensic investigation, and the scope and impact of the attack may take weeks or even months to determine with accuracy, with a high possibility that initial conclusions later may be proven to be incorrect. History has demonstrated that there is a low probability that any entity will have an accurate grasp on the nature and scope of an incident until weeks or months after discovery.

The SEC proposals would require registrants to weigh the need to disclose information about a material cyber security incident as soon as possible to assure deadline compliance and avoid liability against (a) potentially erroneous disclosure of what initially was believed to be a material cybersecurity incident that is subsequently determined to be immaterial, (b) failure to disclose what is not initially believed to be a material cybersecurity incident but that is later determined to be material, and (c) being punished for failing to predict the rapid evolution of knowledge during the initial time immediately following determination of a presumed cybersecurity incident. Moreover, the consequences of being wrong could be severe, particularly where a registrant has an active 1933 Act registration statement that incorporates Forms 8-K by reference and elevates any liability from liability based upon Rule 10b-5 (and similar provisions) to liability based upon Sections 11 and 12.

As a result, we suggest that the Commission provide that any Item 1.05 Form 8-K (and related Form 10-Q and Form 10-K disclosures) be deemed "furnished" and not "filed" for liability purposes. This approach has passed the test of time in other contexts, is appropriate in this context as well, and could result in more disclosure, given "filed" may limit disclosure given the incremental legal liability.

Moreover, there should be no private right of action with respect to Item 1.05 Forms 8-K. We support the Commission's goal to provide for prompt disclosure and transparency, but the Commission should not invite the creation of a new cottage industry of plaintiffs' firms filing class action securities litigation after every cyberattack. We appreciate that the goal of the new rules is to encourage more transparency around cyber incidents. Permitting private rights of action may have the opposite effect, however, by encouraging registrants to wait longer—until they have more certainty about cyber incidents—to avoid lawsuits alleging misstatements where registrants' initial disclosures reflected a misunderstanding, or simply an incomplete early understanding, of the facts. Furthermore, if the Commission's intent is investor awareness or the provisioning of information and not liability, there should be no punishment in the form of private actions for disclosure at the earliest available opportunity. Of course, the Commission always has the ability to enforce its rules as it deems appropriate, as ample investor protections would exist.

We also suggest that the Commission require that any reporting obligations under Item 1.05 of Form 8-K be predicated on a determination of materiality by the principal executive officer, principal financial officer, or senior-most individual employed by a registrant who directly oversees cybersecurity. In reality, individuals working within a registrant's IT operations often will be the first to "discover" a potential incident, but even with the best procedures and training they are not in a position to make a materiality assessment or for a registrant to be bound by any materiality assessment that they might make. The mandatory disclosure obligations in this type of real-time context should reflect that.

Conclusion

As noted above, we commend the Commission for its efforts to enhance cybersecurity disclosures and appreciate the opportunity to comment on the proposals. Given the prominence of cybersecurity risks facing public companies today, it is essential that the Commission issue clear rules on guidance on the matter that carefully balance the value of sharing additional information with investors against the enhanced cybersecurity risks that come with public disclosure of sensitive information. EEI and its officers would be happy to discuss any questions on our recommendations at the Commission's convenience.

Respectfully submitted,

Richard F. McMahon, Jr.
Senior Vice President, Energy Supply & Finance
Edison Electric Institute
[redacted]