1212 New York Ave. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

May 5, 2022

Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549

Comments of the R Street Institute in the Matter of:

A Proposed Rulemaking by the Securities and Exchange Commission: "Governing Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."	))))	File Number S7-09-22

I. Issue summary and summary of the R Street position

The R Street Institute (R Street) is a nonprofit, nonpartisan public policy research organization headquartered in Washington, D.C. Our mission is to engage in policy research and outreach to promote free markets and limited, effective government. The R Street Institute's Cybersecurity and Emerging Threats team focuses on the national security implications of individual, business and government cyber risk. For this reason, the latest Securities and Exchange Commission (S.E.C.) proposed rulemaking is of particular interest to the team.

The proposed rulemaking, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (hereafter the rulemaking) is issued in accordance with the S.E.C.'s mandate to protect investors and ensure the integrity of the securities markets. It is designed to ensure 1) that public companies disclose material cybersecurity incidents in a timely manner; and 2) that public companies disclose the broader details of how and whether they undertake cybersecurity risk assessment, continuity and response programs, and management.

The R Street Institute's Cybersecurity team broadly supports mandatory cybersecurity incident and risk management reporting, and notes that bipartisan lawmakers have called for such a rulemaking.[1] The team believes cybersecurity risk *is* business risk, and that this risk is directly connected to national security—specifically the need to protect U.S. markets from the ever-evolving influx of cybersecurity threats while ensuring economic growth in spite of inevitable cyberattacks.

[1] Jack Reed et al., "Cybersecurity Disclosure Letter," United States Senate, Feb. 8, 2022. https://www.reed.senate.gov/imo/media/doc/cybersecurity_disclosure_letter_to_sec_chair_gensler.pdf.

That said, the team has significant concerns around the current format of the rulemaking, including several items that must be modified, delayed or removed to ensure that the regulations enhance rather than harm overall security; are interoperable with other state and federal government rulemakings on incident reporting; are reasonable obligations for businesses; and provide useful public information for investors.

II. Overview of the proposed rulemaking

The stated goal of the S.E.C.'s reporting requirements is to enable investors to make accurate decisions about the value of a company. Cybersecurity risk is a major component of modern business risk, and thus is integral to understanding whether a company is a safe investment.

The reporting requirements may also help incentivize and equip business and industry to appropriately valuate and prioritize cybersecurity risk management. That is, businesses may be able to take advantage of increased information to better understand how their peers and clients weigh the importance of cybersecurity risk management, and to respond accordingly.

The rulemaking has two major components:

First, to require public companies to promptly disclose to investors if they experience a "material" cybersecurity incident. Specifically, companies would be required to report on such an incident no later than four business days after the finding of materiality (Section II:B); to update the public regularly on new information about previously reported incidents (Section II:C:1); and to disclose to the public any series of cybersecurity incidents that become material in the aggregate (Section II:C:2).

Second, to require public companies to disclose some of the details regarding how they manage and view their own cybersecurity risk. Specifically, companies would be required to disclose how cybersecurity risk is managed and expected to impact overall business operations (Section II:D:1); what, if any, cybersecurity risk assessment, management and continuity of operations/response programs are in place (Section II:D:1); how cybersecurity risk is managed and prioritized by the Board (Section II:D:2); and the level, if any, of cybersecurity expertise of the Board (Section II:E). There are also sections governing how this information should be conveyed to the S.E.C. and how foreign private issuers will be impacted.

As the S.E.C. notes at length, this rulemaking is not the first cybersecurity reporting guidance issued to public companies. It does, however, represent the first formalized rulemaking in this area, as previous issuances have been in the nature of guidance. These rules are necessary, according to the S.E.C., because companies are insufficiently reporting of their own volition or under current guidance; some do not seem to report at all. Others report inadequately or too slowly, and still others may report to different entities or authorities other than the S.E.C.

III. Fundamental considerations

To begin, there are three fundamental considerations that have been raised by other parties in response to the rulemaking. The first is whether the rulemaking conflicts with existing incident reporting passed by Congress, especially the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),

which passed in March 2022.[2] The second is whether it imposes an undue burden on business. The third is whether the information required of companies under the S.E.C. rulemaking provides actionable information for investors.

A. Does the rulemaking oppose congressional intent?

The first thing to ascertain is if the S.E.C. 's rulemaking contradicts the will of Congress by imposing requirements that do not dovetail with Congress' CIRCIA. For example, some argue that Congress favors confidentiality and liability protection for security reasons, and that this should be the main aim of the federal government's rulemaking in this arena. As a reminder, the CIRCIA imposes reporting requirements on critical infrastructure owners and operators within 72 hours to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).[3] It also requires covered entities to report ransomware payments to CISA within 24 hours.

When arguing that the S.E.C. rulemaking undercuts the intent of Congress, critics are generally pointing out that CIRCIA, along with the 2015 CISA Act, provide liability protection and anonymity for companies that report.[4] By contrast, the S.E.C. requires public disclosures for the benefit of investors. Another concern is that the S.E.C. is issuing these requirements before the CIRCIA regulations have even been drafted, perhaps conflicting with future potential regulations.

While the R Street team agrees in part with these concerns, it must be noted that these are different authorities with different goals. CIRCIA is focused on systemic security risk to critical infrastructure. The S.E.C. is focused on ensuring investors have access to full information—for which public disclosure is obviously necessary. Second, there is a deconfliction requirement written into CIRCIA, requiring it to take other measures like those of the S.E.C. into consideration when drafting the new regulations at some point in the next several years.

On the other hand, the S.E.C.'s rulemaking does not align with a trend of private incident reporting focused on improving national security—the most recent example of which is CIRCIA. It also enters a crowded—and contradictory—environment of risk, breach and reporting requirements for U.S. business. This ecosystem includes data breach requirements in existing federal law like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act (GLBA); state privacy and incident reporting laws; agency and sector specific guidelines and regulation; and

---

[2] Mariam Baksh, "Key Lawmaker Defends SEC's Cyber Incident Reporting Proposal," NextGov, March 30, 2022. https://www.nextgov.com/cybersecurity/2022/03/key-lawmaker-defends-secs-cyber-incident-reporting-proposal/363829.

[3] Mary Brooks, "Cyber Incident Reporting: What It Is, Why We Need It, What It Will Fix—and How Congress is Approaching the Issue, Part Two," R Street Institute, Feb. 17, 2022. https://www.rstreet.org/2022/02/17/cyber-incident-reporting-what-it-is-why-we-need-it-what-it-will-fix-and-how-congress-is-approaching-the-issue-part-two.

[4] Ashlie Beringer et. al, "President Biden Signs into Law the Cyber Incident Reporting for Critical Infrastructure Act, Expanding Cyber Reporting Obligations for a Wide Range of Public and Private Entities," Gibson Dunn, March 22, 2022. https://www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities; "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015," Department of Homeland Security and Department of Justice, October 2020. https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf.

others.[5] There are also new proposed incident reporting requirements being discussed and promulgated by other agencies.

B. Does the rulemaking impose an undue burden on business?

The second concern is that the rulemaking could impose a heavy regulatory burden on public companies, while private companies are unaffected. There are, after all, only a few thousand public companies in the United States, while there are millions of privately-held companies that would not have such reporting requirements. [6] However, this is simply not the mandate of the S.E.C. Public companies choose to go public in order to gain access to additional capital from investors. As such, they have an obligation to disclose publicly to their investors. In fact, they are already required to do so, in some circumstances. While the S.E.C. should do its best to minimize the regulatory burden on companies (more on this below), a lack of reporting requirements in one sector does not justify a lack in others.

Of course, this is not to say that private companies are not impacted by cybersecurity incidents and in turn impact the overall security of the United States or the public. In those cases, it will be up to Congress or other entities with authority to pass similar requirements for private companies if they determine there is a security reason to do so. The fact that the S.E.C. is an early mover in this space likely stems from its robust history and mandate to issue regulations—a framework that makes it easier to consider and incorporate cybersecurity requirements, rather than starting from scratch some other industries must.

In short, the United States needs to move from a culture of secretive cyber incident response to a culture of more open and honest communication. Cybersecurity is a collective action problem—and one major way to handle this is by informing the public and raising awareness of cyber incidents to emphasize that this risk impacts everyone. This should be done in a way that is not designed to penalize or publicly shame companies, but rather to incentivize transparency and strengthen cyber practices. The question is whether forced public reporting will contribute to that culture, or alternatively contribute to compliance burden without actually improving transparency, openness and accountability.

C. Does the rulemaking help investors make decisions?

Bipartisan members of Congress have called for measures like that of the S.E.C., writing that investors "have a right to prompt notification of serious cybersecurity incidents. More information will enable investors to hold companies and investment managers accountable."[7] Critics are concerned, however, that while more information can be helpful, it is not clear if investors would actually take a different

---

[5] See, e.g., Health Insurance Portability and Accountability Act. Pub. L. No. 104-191, § 264, 110 Stat. 1936; Gramm-Leach-Bliley Act Pub. L. No. 106-102, 113 Stat. 1338.

[6] Vartika Gupta et al., "Reports of Corporates' Demise Have Been Greatly Exaggerated," McKinsey & Company, Oct. 21, 2021. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/reports-of-corporates-demise-have-been-greatly-exaggerated; Mary Ellen Biery, "4 Reasons Private Companies Matter – A Lot," Verizon, last accessed April 18, 2022. https://www.verizon.com/business/small-business-essentials/resources/4-reasons-private-companies-matter-lot-213549301.

[7] Jack Reed et al. https://www.reed.senate.gov/imo/media/doc/cybersecurity_disclosure_letter_to_sec_chair_gensler.pdf.

investment approach with this information or whether this information would be researched in advance of an investment.

This is a problem the S.E.C. itself touches upon:

> We are unable to quantify the potential benefit to investors and other market participants as a result of the increase in disclosure and improvement in pricing under the proposed amendments. The estimation requires information about the fundamental value of securities and the extent of the mispricing. We do not have access to such information, and therefore cannot provide a reasonable estimate. (Section III:C:1:a(i))

The S.E.C. does not have this information because, as they state, this type of reporting at scale has not been attempted before—as, perhaps, is often the case with new rulemakings. What is already known is that investors do claim a high level of concern over cybersecurity risk, at least in general.[8] Polls have found that cybersecurity is some "investors' foremost environmental, social and governance (ESG) risk."[9] Perhaps most pertinent, research by Ernst & Young has found that:

> Because the threat of a breach cannot be eliminated, some investors stressed that they are particularly interested in resiliency, including how (and how quickly) companies are detecting and mitigating cybersecurity incidents. Some are asking their portfolio companies about specific cybersecurity practices, such as whether the company has had an independent assessment of its cybersecurity program, and some are increasingly focusing on data privacy and whether companies are adequately identifying and addressing related consumer concerns and expanding regulatory requirements.[10]

It would be helpful to know whether the S.E.C. has conducted any research into investors' priorities and decision-making processes in this area, and what those preliminary results were. At this point, we urge a cautious and slow approach to the rollout of this rulemaking, given that the expected costs to business are higher than the currently known benefits for investors.

In summary, each of these points above has merit, but the team believes the need to provide greater transparency for investors and the public is also important. We are confident that the spirit of the S.E.C.'s rulemaking can be modified to address these concerns and blunt the worst of them. We do suggest, however, that the S.E.C. delay finalization of the proposed rule for some months to better understand the implications on business and on security, and that, when implemented, there is a delayed uptake process or grace period to allow businesses to prepare themselves for the new requirements.

---

[8] See, e.g., "Cyber Disclosures Reveal Varying Levels of Transparency Across High-Risk Sectors," Moody's Investors Service, Oct. 2, 2019. https://journalofcyberpolicy.com/wp-content/uploads/2019/10/Moodys-Cyber-disclosures-10.19.pdf; Beatrice Peterson, "Wall Street Eyes Cybersecurity, with Goldman Sachs Announcing $125 Million Investment," abcNews, April 20, 2022. https://abcnews.go.com/Business/wall-street-eyes-cybersecurity-goldman-sachs-announcing-125/story?id=84091514.

[9] RBC Corporate Governance and Responsible Investment Team, "Cyber Security is the Top ESG Concern for Institutional Investors," RBC Global Asset Management, Feb. 12, 2020. https://www.rbcgam.com/en/ca/article/cyber-security-is-the-top-esg-concern-for-institutional-investors/detail.

[10] Steve W. Klemash et. al, "What Companies are Disclosing About Cybersecurity Risk and Oversight," Harvard Law School Forum on Corporate Governance, Aug. 25, 2020. https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight.

IV. Point-by-point considerations

While we support the overall spirit of the rulemaking as drafted, there are a few considerations that must be addressed before the rulemaking is finalized.

**Note that the headings and numbering below directly reference the S.E.C. rulemaking.*

B. Reporting of Cybersecurity Incidents on Form 8-K

3. Could any of the proposed Item 1.05 disclosures or the proposed timing of the disclosures have the unintentional effect of putting registrants at additional risk of future cybersecurity incidents?

Potentially, yes. See points 4, 6, 7 and 10, below.

4. Should we modify the timeframe in which a registrant must file a Form 8-K under proposed Item 1.05?

Yes. While investors could possibly benefit from the reporting of "material" cybersecurity incidents on Form 8K, their needs should be balanced with other priorities, namely accuracy, security and privacy, as well as creating the least burdensome environment for companies. A four-business day deadline from the finding of materiality is simply too short for multiple reasons:

- Accuracy:
  - It may cause undue harm or panic, as many of the questions identified in 1.05 will likely not be figured out within four business days. That could decrease the overall integrity of the incident reporting process.
  - Perversely, it could incentivize companies to intentionally delay finding something to be "material" despite the "as soon as reasonably practicable after discovery" language (p. 22).
- Security:
  - It may expose technical details unwittingly, as teams do not yet know what is important and what is not. It may also force a company to notify investors of a breach before systems are patched or otherwise configured securely—something that could also implicate other companies in a supply-chain breach.
  - It may interfere with law enforcement and related investigations into a given incident, whether at a local level or with the FBI or CISA.
- Privacy:
  - If individuals' personal information is compromised in an incident, a company could potentially have to prioritize warning investors before warning victims. This is the wrong order as affected users often need to take immediate action over their breached information.
- Burdensome:
  - It places too heavy of a burden on reporting an incident while teams are still endeavoring to identify the full extent of harm, ensure continuity of operations and remove the threat.

It is important to balance transparency with truth-finding, security and privacy. The best way to do this is to extend the deadline for public disclosure. A deadline of 15 business days is more reasonable but

still ensures timely disclosure—after all, current reporting times range from many weeks to even months.[11] The S.E.C. could also implement a cure period to allow businesses a defined period of time to fix potential reporting mistakes, which could be perpetual or for the initial stages of the reporting requirement. This would allow businesses an opportunity to comply rather than facing enforcement over what might be a simple mistake.

5. Should there be a different triggering event for the Item 1.05 disclosure, such as the registrant's discovery that it has experienced a cybersecurity incident, even if the registrant has not yet been able to determine the materiality of the incident?

No. "Material" impact is a good metric that will differ from company to company. Imposing, as suggested in Question 5, a quantifiable threshold determined by affected asset percentage or cost is unproductive. For example, one company might face higher monetary losses from a cyber incident, but a second company's breach that has a lower rate of loss but a business model that relies on data integrity—such as an online verification platform—is critical for an investor to know about. That said, the S.E.C. 's definition of what is material is not clear and should be better defined in the rulemaking—particularly to prevent companies taking advantage of delaying a material determination in order to avoid reporting or for companies inadvertently not complying because of a misunderstanding or lack of clarity.

6. To what extent, if any, would the proposed Form 8-K incident reporting obligation create conflicts for a registrant with respect to other obligations of the registrant under federal or state law?

Yes—but the extent is not clear. Not all conflicts are problematic, and some are yet to be determined (for example, the above-mentioned need for CISA to build out CIRCIA requirements). Some, however, may pose a privacy or security concern. Take, for example, the following hypothetical: a major public company that stores private health information is breached. Under the Health Insurance Portability and Accountability Act (HIPAA), the breach must be disclosed to victims within 60 days.[12] Thus, there is the potential for investors to know about a breach of confidential health information before victims are aware. There is furthermore the potential for criminals to take advantage of the knowledge that there has been a breach but that victims have not yet been informed. The same could be said for state privacy laws, which mandate reporting of incidents across very different timelines.

Of course, these other delays are not the responsibility of the S.E.C and this should not be an excuse to avoid public reporting. However, the S.E.C. should much more aggressively deconflict with other reporting requirements before passing this rulemaking, given the situation. Again, extending the four-business-day reporting period will also help here.

7. Should any rule provide that the Commission shall allow registrants to delay reporting of a cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security?

---

[11] Jake Olcott and Maham Haroon, "From Months to Minutes: Can New Regulations Accelerate the Cyber Incident Disclosure Process?," BitSight, March 29, 2022. https://www.bitsight.com/blog/months-minutes-can-new-regulations-accelerate-cyber-incident-disclosure-process.

[12] Office for Civil Rights, "Breach Notification Rule," U.S. Department of Health & Human Services, July 26, 2013. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

Yes. While the excuse of an "investigation" has for too long been used to obfuscate the details of cybersecurity incidents, there are major reasons why exceptional security circumstances should justify a delay.

+ Investigators may not want to tip off criminal or state actors to the fact that their operations into U.S. systems have been discovered—a revelation that could cause these actors to hide or otherwise bide their time and make remediating the attack more difficult.
+ Information could harm diplomatic or strategic efforts being led by the U.S. government.
+ Reporting may interfere with classified internal government discussion and decisions on attribution if the breach was perpetrated by a nation state adversary.
+ Reporting may cause evidence related to a criminal investigation to be compromised or lost.

In short, the Attorney General must be allowed to ask for a reporting delay. In fact, it may be better to allow a similar determination to also be made by CISA, the FBI, the office of the National Cyber Director, the National Security Council and/or the Intelligence Community. Nevertheless, such a determination should be extraordinary rather than routine.

10. As described further below, we are proposing to define cybersecurity incident to include an unauthorized occurrence on or through a registrant's "information systems," which is proposed to include "information resources owned or used by the registrant." Would registrants be reasonably able to obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them?

In some cases, yes. It appears that it will depend on 1) how well the third-party compromise is understood (or even if the third party discloses a breach or compromise at all); and 2) how well the given public company understands its own assets and liabilities. It seems likely that companies have direct control over the second dependency, and that they will require new acquisitions and contract language to ensure the first dependency is met.

One point to consider more fully is whether this could potentially worsen a broader supply chain compromise. If a public company is required to disclose an incident involving a third-party provider within four days, that may preempt the third-party provider's own reporting obligations, ability to issue a patch, or ability to ensure that the patch or other mitigative measures have been implemented.

Thus, compromises of third-party providers should perhaps be handled separately from the proposed new process to avoid worsening a supply chain incident. If possible, a security screening might be added prior to the publication of third-party-related compromises. This could help mitigate security risks.

11. We are proposing that registrants be required to file rather than permitted to furnish an Item 1.05 Form 8-K. Should we instead permit registrants to furnish an Item 1.05 Form 8-K, such that the Form 8-K would not be subject to liability under Section 18 of the Exchange Act unless the registrant specifically states that the information is to be considered "filed" or incorporates it by reference into a filing under the Securities Act or Exchange Act?

No. This wording is not particularly clear, but it is our position that this should be a mandatory rather than a voluntary exercise. We reiterate our concerns about the short timeline, several vague definitions and no exceptions for law enforcement or national security considerations.

C. Disclosure about Cybersecurity Incidents in Periodic Reports

15. Should we require registrants to disclose any material changes or updates to information that would be disclosed pursuant to proposed Item 1.05 of Form 8-K in the registrant's quarterly or annual report, as proposed?

Yes. Ongoing reporting is perhaps even more important than the initial disclosure, as it signals to investors which companies have security procedures in place to ensure continuity of operations, protect from further intrusion and return to business-as-usual.

16. Should we require a registrant to provide disclosure on Form 10-Q or Form 10-K when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate, as proposed? Alternatively, should we require a registrant to provide disclosure in Form 8-K, rather than in a periodic report, as proposed, when a series of previously undisclosed and individually immaterial cybersecurity incidents becomes material in the aggregate?

Yes—on Form 8K. In the same way that materiality is determined for an individual incident and required to be reported on Form 8K, so too should aggregate incidents be reported. However, first the S.E.C. should more clearly define what constitutes materially aggregate instances and provide strong examples thereof. Notably, cybersecurity incidents are so unfortunately common that a strict reading of this section could cause overreporting to the point that it is meaningless for shareholders. The worst thing to do is to overload the system with information that is not analytically meaningful.

D. Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks

17. Should we adopt Item 106(b) and (c) as proposed?

Generally, yes. Investors can and should know the ongoing steps that a company is taking to manage cybersecurity risk. Businesses may also benefit from a transparent accounting of how other companies are prioritizing cybersecurity. However, this needs to be balanced so that details that could compromise an entity's security posture are not required. For example, precise information on how entities protect themselves, what products they use or how they plan to respond to a cyber incident could be exploited by a bad actor. Businesses may even be targeted if an actor determined they have weak cybersecurity measures in place.

For this reason, the S.E.C. needs to be specific about the level of detail expected in reports and ensure overly sensitive data is not provided for public disclosure. As one example, there is a difference between answering whether "the registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents" with a simple Yes/No and needing to provide specific measures about how incidents are detected.

19. The proposed rule does not define "cybersecurity." … Would defining "cybersecurity" in proposed Item 106(a) be helpful?

Yes. This is a rulemaking on cybersecurity. A common definition seems necessary. The S.E.C. should use the definition provided by CISA: "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."[13]

22. Are there 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?

Generally, no. Obviously, companies should not give detailed descriptions of software or step-by-step response policies, but this disclosure inquiry is an iteration of the tired argument that "security by obscurity" is helpful. This idea is outdated. Keeping secret about a lack of preparedness does nothing but enable bad habits and patterns to continue. However, a one-year grace period might be offered to companies before reporting requirements come into effect in order to ease the transition.

E. Disclosure Regarding the Board of Directors' Cybersecurity Expertise

26. Would proposed Item 407(j) disclosure provide information that investors would find useful? Should it be modified in any way?

Unclear. It is not clear to us how this information benefits investors or how cybersecurity expertise on the Board is more beneficial than other measures—such as ensuring that cybersecurity risk is thoroughly communicated to the Board; that it is incorporated into strategy; and that decision makers at the highest levels are held accountable for cybersecurity failures.

V. Request for clarification

In addition to the points above, there is a further question that the team does not believe has been clearly addressed in the rulemaking:

Can information in these filings be used as evidence to hold a company liable in related or unrelated criminal or civil cases?

The S.E.C. should affirmatively say that this information should not be used for enforcement actions unless a company willfully does not comply with these disclosure agreements. The goal of this rulemaking is to increase transparency and public knowledge about the management of business risk—not to penalize businesses.

VI. Conclusion

In conclusion, the R Street Cybersecurity team supports the S.E.C's efforts to improve public information around cybersecurity incidents and the risk management decision making processes of public companies. Nonetheless, there are several components that should be revisited in order to ensure that

[13] Cybersecurity and Infrastructure Security Agency, "Security Tip (ST04-001)," Department of Homeland Security, Nov. 14, 2019. https://www.cisa.gov/uscert/ncas/tips/ST04-001.

the regulations enhance rather than harm overall security; are interoperable with other state and federal government rulemakings on incident reporting; are reasonable obligations for businesses; and provide useful public information for investors.

Respectfully submitted,

_____

The R Street Cybersecurity Team
Point of Contact: Mary Brooks
[redacted]
Fellow
R Street Institute
1212 New York Ave. NW,
Suite 900
Washington, D.C. 20005