U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

Via rule-comment@sec.gov

May 9, 2022

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

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22)

Dear Ms. Countryman:

The U.S. Chamber of Commerce welcomes the opportunity to comment on the Securities and Exchange Commission's (the SEC's or the Commission's) *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* proposal.[1] We appreciate the engagement that the Chamber has had with the SEC on this complex issue.

The Chamber agrees with the Commission that responsible cybersecurity policies and practices are in the best interest of investors, boards of directors, and management. However, any cybersecurity disclosure policies must abide by the norms of materiality and the SEC's legal mandate to promote investor protection, competition, and capital formation. As it stands, the Chamber contends that the proposed rules have several significant flaws:

- The Commission's proposal conflicts with the policy goals established by Congress in recent cybersecurity legislation, including the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which requires certain critical infrastructure entities to report on a confidential and protected basis covered cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours.

- The SEC's proposed rules leave businesses in the unenviable position of facing conflicting cybersecurity reporting directives from several U.S. agencies. The Chamber believes that there needs to be more assertive harmonization of cybersecurity incident reporting policies to enable businesses to understand and follow clear, consistent guidelines and processes.

- The public disclosure of a company's cybersecurity policies and practices, as envisioned by the SEC proposed rules, could provide a roadmap for bad actors and hostile nation states from which they can attack businesses. Such disclosure degrades investor protection and harms competition and capital formation.

- The SEC has failed to provide industry with the opportunity to fully assess and comment on the costs and benefits of its proposal. A basic review of the proposed rules indicates that this is an economically significant rulemaking, and it should be subject to an enhanced economic analysis of the expected costs.

Accordingly, the Chamber believes that the current proposal has severe deficiencies requiring the SEC to reassess the proposal and hold a roundtable with stakeholders, including investors, business groups, and government entities, to identify key issues and solutions. The Chamber trusts that such a deliberative approach could yield disclosures related to cybersecurity that stand the test of time and enable the SEC to meet its legal mandate. We look forward to working constructively with the SEC to achieve those goals.

***

The remainder of this letter consists of business community feedback to some of the key themes and questions put forth in the Commission's rulemaking. The Chamber does not attempt to answer each question that the SEC asks. On May 2, 2022, the Chamber urged the SEC to extend the comment period by an additional 45 days, but the Commission disagreed.

The complexity of the SEC's cybersecurity rulemaking warranted additional time for at least three reasons:

- The Commission's proposed amendments include an array of reporting, risk management and strategy, and governance topics that are highly detailed and would have important impacts on publicly traded companies, investors, and U.S. economic and national security (e.g., public-private partnerships). Alone, this section covers some 40 questions for commenters.

- The economic analysis portion of the rule covers many lengthy and intricate studies (some of which are not freely available to the public) that the stakeholders deserve time to thoroughly analyze in formulating responses to the rulemaking. Indeed, the Commission has not attempted to calculate any quantitative values for benefits of the proposed rule. Moreover, the benefits are only described in vague qualitative terms.

- In addition to this cybersecurity rulemaking, the Commission is promulgating several other rules affecting the business community that have overlapping comment periods and divide the time and attention of industry professionals. The SEC's decision to put forth multiple proposals, combined with short comment periods, raises concerns about the adequacy of the Commission's rule-writing process.[2]

***

In 2018, the Commission issued interpretive guidance to reinforce and expand upon its staff-level guidance released in 2011.[3] In both interpretive guidance documents, the Commission addressed the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity. The proposed rules state that while companies' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved in the wake of the interpretive guidance, disclosure practices remain inconsistent.

The SEC's proposed amendments would require near real-time and periodic reporting of material cybersecurity incidents. The Commission is also proposing changes that would require disclosures about a company's policies and procedures to address cybersecurity risk; management's role and expertise in implementing a company's cybersecurity policies, procedures, and strategies; and the board of directors' oversight role and its expertise pertaining to cybersecurity. The SEC's proposed rules, in short, would include these important changes to the Commission's reporting requirements:

- Require current reporting about material cybersecurity incidents on Form 8-K within 4 business days of a materiality determination.

- Require periodic disclosures regarding, among other things:

    - A registrant's policies and procedures to identify and manage cybersecurity risks.
    - Management's role in implementing cybersecurity policies and procedures.
    - A board of director's cybersecurity expertise, if any, and its oversight of cybersecurity risk.
    - Updates about previously reported material cybersecurity incidents.

The Chamber recognizes the SEC's legal obligation to protect investors, promote competition among companies, and further capital formation—but its proposed cybersecurity rules overreach by casting an unnecessarily wide net for company information. The practical realities of cybersecurity should help inform the SEC that increased cybersecurity incident disclosures would likely translate into heightened risks for companies and their investors—the exact opposite of the Commission's policy goal.

Key Points

- The intent of the SEC's proposed disclosure regime rests on furthering investors' knowledge of companies' cybersecurity risk management postures. But the Commission should not override laws and regulations related to cybersecurity and protected disclosures, thoughtfully considered delays in reporting, among other polices.

- The Chamber supports responsible and protective cybersecurity reporting to the government, consumers, and investors, but we oppose the SEC's proposed rule in its current form. It runs counter to sound cybersecurity policies and practices.

- The Chamber is open to working with the Commission to develop a rulemaking that prioritizes harmonization with other federal agencies and provides timely information to investors while mitigating risks associated with disclosing sensitive cybersecurity information to the public.

- The SEC should work with other federal agencies and cybersecurity policymakers, including the national cyber director (NCD), to better coordinate its proposed amendments with other federal reporting/disclosure/notification laws and requirements.

- The costs of the rulemaking appear on its face to outweigh its benefits—which remain uncertain—to investors.

- The SEC has not acknowledged the need for targeted delays in reporting. Companies need time to conduct internal investigations to accurately determine an incident's true scope and impact or partner with law enforcement and/or national security agencies on investigations.

- The Chamber is concerned that the SEC's proposed rules could push companies to prioritize making premature, compliance-based disclosures over remediating cybersecurity incidents, thus jeopardizing shareholder returns.

- Companies are concerned that the requirements mandating the early disclosure of incident and vulnerability information could undermine the security of their enterprises and their shareholders. Such requirements would sharply contrast with industry best practices and government incident and vulnerability response playbooks.

- The proposed rules would require an unprecedented micromanagement of companies' cybersecurity programs and their boards. The Chamber is not convinced that investors are demanding increased intervention regarding companies' plans to detect, respond to, and recover from online incidents. The Commission has neither adequately explained how its proposed rules would protect investors nor justified their costs against the purported benefits.

- The scope of the SEC's definition of a "cybersecurity incident" is too expansive. Material cybersecurity disclosures should correspond to significant incidents that do actual harm. Getting the definition of a cybersecurity incident correct requires more time than the SEC's comment period allows.

- The Chamber believes that the SEC's 2018 interpretive guidance is effective in instructing publicly traded companies regarding their cybersecurity-related reporting obligations, including appropriately informing investors.

1. Common Ground Is Achievable on Disclosure Policy—But Not at the Risk of Company Security, Which Would Harm Investor Interests

The Chamber agrees with the SEC that cybersecurity incidents can impact the economy and publicly traded companies (companies or registrants). Companies of all sizes

and sectors, like government entities, are susceptible to cybersecurity incidents. The business community is working diligently to respond to and mitigate these risks. Senior managers and boards are both increasingly concerned about cybersecurity threats and are taking concrete steps to protect their information systems and digital assets.

The Commission's 2018 interpretive guidance helps companies understand their cybersecurity-related reporting obligations, including the importance of policies and procedures and the application of insider trading prohibitions.[4] The Chamber is committed to working with the SEC to craft consistent, useful, and timely company disclosures on registrants' material cybersecurity incidents and security programs to better guide investors. We agree with Chair Gary Gensler's view that "[a] lot of issuers already provide cybersecurity disclosure to investors," and that "companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."[5]

While the SEC's proposed rules are predicated on our shared goals of meeting investor interests and responding to the evolving cyber landscape, disclosure rules should not reduce or put at risk companies' security and resilience against criminal groups and foreign hackers and/or their proxies. As written, the proposed rules prioritize disclosures, which may or may not be useful to investors, over cybersecurity risk management. This approach would not protect shareholders and could have the opposite effect by putting companies in jeopardy by forcing them to allocate resources toward compliance-based reporting rather than triaging the complex elements of identifying and resolving cybersecurity incidents. The disclosure of vulnerability data, if shared prematurely, could actually enable attackers.

Moreover, by requiring companies to disclose the nature of an attack before it is resolved, a disclosure of vulnerability data could actually enable attackers. This is not in the interest of the company or its shareholders and, therefore, the proposed rules miss the mark on investor protection. The Commission should focus on coordinating with other federal agencies on incident reporting where appropriate instead of creating a new regulatory regime that would contradict, if not undermine (e.g., in the case of law enforcement and national security investigations) the work of other government entities.

2. Chamber Policy Emphasizes Collaborative and Protective Programs

The Chamber's cybersecurity policy baseline informs our views on congressional and executive branch policymaking and negotiations. In March 2021, the Chamber released a paper that highlights our thinking on some key cybersecurity themes and issues. The paper's topics are summed up in 7 words—potential, program, protection, preemption, partnership, price, and promotion. It guides the Chamber's evaluation of cybersecurity legislation and regulations, including the SEC's proposed amendments, to negotiate policy outcomes that address multiple stakeholder (e.g., government and private sector) interests.

A missing element in the SEC's synopsis of the global cybersecurity environment is the prominent role that foreign nation states and their proxies play in conducting illicit operations against companies and U.S. interests. Businesses are subject to relentless, often state-sponsored, cyberattacks without effective government protection. Cyberspace remains the

only domain where we ask businesses to defend themselves against foreign powers and/or their surrogates.[6] Among other things, the Chamber believes that this security gap justifies blending any new cybersecurity requirements with regulatory and legal protections.

2.1 Workable Cybersecurity Reporting Bills Run Counter to the Proposed Rules

The Chamber supports responsible cybersecurity reporting to the government, consumers, and investors. Indeed, we have advocated for policies that require industry disclosures to agencies on a number of cybersecurity matters. Notable examples include the Cybersecurity Information Sharing Act of 2015 (CISA 2015); the CISA administrative subpoena law; and CIRCIA, which was recently signed into law.

- **CISA 2015.** The Chamber formed and led the 50-association Protecting America's Cyber Networks Coalition to pass CISA 2015 to promote business security and resilience against cyberattacks. The SEC should not overlook that industry championed this legislation in the face of considerable opposition from some parties to fundamentally improve information-sharing practices between the U.S. government and the business community.

  A primary goal of CISA 2015 remains alive and well—that is, to motivate businesses to share cyber threat data with both industry peers and government entities to bolster our critical infrastructure, lifeline, first responder, and business systems.[7]

- **CISA administrative subpoena law.** The Chamber worked closely with Congress to develop and pass the Cybersecurity Vulnerability Identification and Notification Act of 2020 (S. 3045).[8] This bipartisan law grants CISA new administrative subpoena authority to identify and address a vulnerability in a covered device or system that supports critical infrastructure. The Chamber was cognizant of enabling CISA to accomplish its objectives as a cybersecurity risk adviser.

  S. 3405 was tailored to protect sensitive business information from public disclosure. Both bill writers and industry groups expressed concerns that information collected by CISA under the legislation could get disseminated publicly (e.g., to the media), thus revealing the identity of at-risk entities to bad actors.[9] Congress recognized the importance of privacy and civil liberties protections when writing S. 3045. Lawmakers also wanted to ensure that the identity of at-risk entities would only be disclosed to law enforcement or a national security agency with the consent of the at-risk entity.

The Mitigation of Security Vulnerabilities Should Be Handled Discreetly, Not Publicly

S. 3045 limits CISA's ability to disclose any non-public information it obtains as a result of the administrative subpoena with its Federal and non-Federal partners. Similar authorities have been the subject of misuse by other Federal agencies, and as such the authorities granted in this bill are meant to ensure that CISA's compulsory authority is used strictly to enhance the cybersecurity of the nation's critical infrastructure. To ensure that this authority is not used as the basis for law

> enforcement or regulatory action, S. 3045 requires any entity identified in the subpoena to be notified within seven days.
>
> —Excerpt from the Senate Homeland Security and Governmental Affairs Committee report to S. 3045, July 29, 2020[10]

- **CIRCIA.** The Chamber devoted much of 2021 to helping Congress write and pass this cybersecurity incident reporting law.[11] To spotlight workable policy, it is useful to assess elements of the SEC's proposed cybersecurity rules against CIRCIA—which doesn't make for simple comparisons. Congress put a premium on protecting incident data from unwarranted disclosure. Congress also clarified that to the extent any vulnerability information is shared as part of the covered cyber incident data, it needs to be handled based on principles consistent with international standards and industry best practices requiring protection and strict confidence.[12]

CIRCIA's restrictions on government use of data closely align with CISA 2015, including provisions to do the following:

- Prohibit federal and state governments from using submitted data to regulate reporting entities.
- Treat reported information as commercial, financial, and proprietary.
- Exempt reported information from federal and state disclosure laws.
- Preserve trade secret protections and any related privileges or protections.
- Waive governmental rules related to ex parte communications.

Subject to a forthcoming rule led by CISA, CIRCIA requires certain owners and/or operators of critical infrastructure to report "covered cyber incidents" to CISA within 72 hours. (The law also compels these entities to report ransomware payments to CISA within 24 hours of making them.) While this reporting timeline is relatively short, the new CIRCIA requirements codify important safeguards for companies in reporting cybersecurity incident information, a significant one being the confidential nature of the reporting.

3. The Economic Analysis Is Insufficent for Commentors to Appropriately Understand the Costs and Benefits of the Proposal

The SEC has not provided commenters with a sufficient and specific analysis of the costs, burdens, economic impact, and benefits of the proposed rules. The truncated comment period—especially given a complex proposal of this size and the volume of other proposals that are out for comment—has not allowed the Chamber and its members to sufficiently assess the rulemaking's costs and benefits. The Commission has not allowed for an appropriately timed process to consider and comment on the financial and policy pros and cons of its proposed amendments.

A simple read of the Commission's proposal shows that the costs of the rule meet the triggering thresholds for an economically significant rulemaking under the Unfunded Mandate

Reform Act of 1995 and the Small Business Regulatory Enforcement Fairness Act. The Chamber requests that the SEC undertakes an enhanced economic analysis as required by law for economically significant rulemakings. Additionally, we would request that such an analysis be released for appropriate review and comment under the Administrative Procedures Act.

Given the likelihood that the costs of the proposed rule would be in the hundreds of millions of dollars, it is crucial that the benefits be analyzed in quantitative detail. Failure to do so risks adoption of a regulation for which the costs far outweigh any reasonable estimation of the benefits. With the total initial yearly costs likely $317.5M to $523.4M ($38,690 to $69,151 per regulated company), and future annual costs of $184.8M to $308.1M ($22,300 to $37,500 per company), it is doubtful the Commission's evaluation that the discounted present value of benefits to investors would reasonably exceed the discounted present value of the costs.

4. Reporting Material Cybersecurity Incidents: The Mandatory 4-Day Window and the Level of Detail Required Raise Legitimate Security Concerns[13]

Under its proposed rules, the Commission would amend Form 8-K to add Item 1.05 to require a company to disclose information about a cybersecurity incident within 4 business days after the company determines that it has experienced a "material" cybersecurity incident. The SEC argues that such reporting would "significantly improve the timeliness of cybersecurity incident disclosures, as well as provide investors with more standardized and comparable disclosures." Specifically, a company would be required to disclose the following information about a material cybersecurity incident at the time of the Form 8-K filing:

- When the incident was discovered and whether it is ongoing.
- A brief description of the nature and scope of the incident.
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose.
- The effect of the incident on the registrant's operations.
- Whether the registrant has remediated or is currently remediating the incident.

The SEC contends that it "would not expect a registrant to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." However, it is difficult to square the SEC's assurances to industry with the proposed mandate for registrants to disclose more data about a material cyber incident within 4 business days.

The mere *fact* of a premature or overly hasty disclosure of information, including regarding potential system vulnerabilities, would likely give attackers advantages over defenders. As the SEC recognizes, such disclosures would conflict with industry best practices and international standards for coordinated vulnerability disclosure (CVD).[14] Almost any public detail can provide clues to malicious actors, especially if they are combined with other unknown information (e.g., a zero-day exploit). While an incident is ongoing, companies

should not be put in the position of having to determine which details are sufficiently vague and/or how a corresponding disclosure could negatively impact the online ecosystem at large.

At a minimum, hurried disclosures could result in incorrect information being shared with investors. Confidential information about a registrant's technical security program could place it at increased risk because of a rushed push to disclose without adequate time to evaluate the substance of what is being disclosed.

The SEC says that in some instances, the timing of the company's materiality determination "may coincide with the date of discovery of an incident," but in other cases, the materiality determination would be made after the discovery date. The Commission stresses that it expects registrants to be "diligent in making a materiality determination in as prompt a manner as feasible." The Commission adds that "'a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident.'"

Rather than using the time sensibly to mitigate a cybersecurity incident before details are revealed openly, the proposed rules indicate that a company may prefer to delay making a materiality determination to evade its disclosure requirements. The Commission should carefully consider which priority matters more—protecting investors via effective cybersecurity incident mitigation or openly disclosing an incident that has not been fully remediated.

The Chamber opposes cybersecurity disclosure policies that would place a victim—and, by extension, the value of its shareholders' investments—at an elevated risk of further victimization because the details surrounding a cybersecurity incident are prematurely made public, particularly if an incident has not been resolved. Furthermore, the Commission has not incorporated an exception to temporarily delay reporting of material incidents in cases where disclosures could negatively impact national security equities and/or law enforcement investigations against illicit hackers.

The Chamber agrees that information should be disclosed to investors in a timely and practical manner to assist investors' decision making. Equally important, however, is the importance of safeguarding company, consumer, and shareholder data, particularly in in reports to government entities. Companies rightly guard against exposing system vulnerabilities, which can affect not only the cybersecurity of users but registrants and the wider internet ecosystem.

Government officials routinely advocate for strong cybersecurity and the importance of safeguarding of data—the Department of Defense's Cybersecurity Maturity Model Certification program is one of many examples that come to mind—and yet the Commission's proposed rules seem contrary to these goals. The Commission should not impede companies' ability to safeguard sensitive cybersecurity and (in some cases) national security information.[15]

4.1 The SEC's Rules Need to Accommodate Temporary Delays

The Chamber is concerned that the proposed rules would not authorize a temporary reporting delay because of a company's ongoing internal investigation or an external investigation, including one with or by law enforcement—which often directs a company not to disclose the nature of an investigation to avoid compromising an ongoing case. The Commission cites its 2018 interpretive guidance to noting that while an investigation could affect the specifics in a company's disclosure, "an ongoing internal or external investigation—which often can be lengthy—would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." The Commission adds that any delay in reporting would "undermine" its policy goal of "providing timely and consistent disclosure of cybersecurity incidents" to investors.

The Chamber believes that this view is counterproductive. Delays would not undermine the Commission's policy objectives—just the opposite. The SEC should be actively urging companies to work with law enforcement to mitigate cyber incidents—including granting prudent reporting delays—to help companies' security and financial positions, which ultimately benefits investors. The Commission contemplates whether the proposed rules should provide for a delay in reporting based on a request from the U.S. attorney general (AG). The SEC's proposal must accommodate both the AG and appeals from industry and law enforcement more broadly.

The Commission needs to accommodate the AG and appeals from industry working in tandem with law enforcement more broadly. The Commission should expand the authority to delay public disclosure beyond the AG to other corners of government with jurisdiction over cybersecurity investigations. The Commission has been too parochial in its suggestion that only the AG has the requisite authority or expertise to intervene. The Chamber urges the SEC to develop a more workable process by which other appropriate government officials can prompt a reporting delay in consultation with the SEC. The fact of a rushed public disclosure of an incident—including an unpatched vulnerability—could alert a range of bad actors (e.g., criminals and nation states) to identify and attack other victims, which could lead to additional cyberattacks within and cross industries.

Similarly, issues related to public safety should be considered for certain critical industries. A premature disclosure of vulnerabilities in the automobile, airplane, and/or medical device sectors could cause unmerited panic. Premature disclosure could cause individuals to make safety-related decisions based on incomplete information, such as deferring medical procedures or disconnecting certain types of devices from the internet. It can take significant time and effort, often alongside government authorities, to not only determine the appropriate fix for vulnerabilities but allow it to be done safely. Particularly in the health care space, patient safety must be the top concern with any cybersecurity vulnerability, and policymakers must not inadvertently impact patients in the rush to disclose material cybersecurity incidents.

As written, the proposed rules could damage the public-private partnerships that industry and the public sector have spent years cultivating, including at the government's behest through energetic information sharing programs. The SEC's proposed rules need to allow a reporting delay per a request from law enforcement below the level of the AG or another agency (e.g., a sector risk management agency) that is authorized by law to conduct cybersecurity investigations if the affected company gives its consent to authorities.

To the extent that the SEC is considering proposing the disclosure of information revealing vulnerabilities, such a policy would be inconsistent with international standards and industry best practices for CVD. Such a requirement would conflict with federal legislation, including apparently requiring federal contractors to follow the SEC's rather than contracting agencies' rules. Vulnerability information needs to be protected until mitigations are in place, a view that has wide consensus. In short, the Commission's proposed amendments would likely create an unworkable conflict between the SEC and other agencies on CVD. Registrants could be put in the position of either following the Commission's rules or protecting users by not disclosing vulnerability information based on international standards and industry best practices.

Many state data breach reporting laws allow a covered organization to delay notification if law enforcement concludes that such notice would impede an investigation. State laws also may allow a victim company to forgo providing notice altogether if the victim company consults with law enforcement and determines that the breach would not likely result in harm to the individuals whose personal information has been acquired and accessed. It is also noteworthy that companies that cooperate with law enforcement may be viewed more favorably by regulators looking into a data breach. While it may not be the Commission's intent, the rulemaking could turn company and law enforcement cooperation on its head.[16]

By requiring the disclosure of a material cybersecurity incident 4 days after a determination, the Form 8-K filing could precede—or almost preempt—data breach notices to state attorneys general, individuals, and potentially impacted business partners. Further, providing such details prior to the completion of a forensic investigation would likely expose companies to litigation before it has a full picture of the impact of a cybersecurity incident and undermine attorney-client and work product privileges associated with investigating the cybersecurity incident.

The Chamber agrees with a letter written by several financial services sector associations, led by the Bank Policy Institute. The letter says, "All 50 states have passed laws authorizing delayed disclosure to consumers of breaches of their sensitive personal data at the request of law enforcement to avoid compromising an ongoing investigation." The Gramm-Leach-Bliley Act similarly authorizes such delayed disclosure by financial institutions, and federal law enforcement agencies make such requests of registrants in appropriate circumstances.[17] The groups emphasize, "Without a corresponding law enforcement exception, the [SEC's proposed rules] would undermine the determination of all U.S. states and numerous federal agencies that law enforcement's need to protect the public weighs in favor of a disclosure delay in limited circumstances."

In addition, the Chamber frequently hears from the FBI and the Secret Service that notifying them is key toward mitigating cybersecurity incidents. Authorities can often figure out the details of a cybersecurity incident—the what, the when, and the how—as the incident moves forward. But the advantages of time and dialogue are crucial assets.

The proposed rules note that in some cases the timing of a company's materiality determination could coincide with the date of discovery of an incident. Therefore, the importance of a company partnering with law enforcement, including being granted a temporary reporting delay, takes on added significance. Yet in other cases, decision making about materiality would come after the discovery of a cybersecurity incident.

In either case, companies need time—more than a handful of business days—to provide law enforcement with some core information, including the following:

- The victim's name.
- The earliest date of known malicious activity.
- What information or assets have been impacted
- What, if any, data was stolen or exfiltrated.
- Whether a ransom has been demanded, including having some mechanism in place (e.g., a digital wallet) for the ransom to be paid.

Law officers tell the Chamber that well-informed answers to these questions help them properly understand the threat picture and effectively scale the government's response. The proposed amendments would likely undercut important strides in public-private cooperation that the excerpt below from a November 2021 Department of Justice press conference on the Sodinokibi/REvil Ransomware arrest highlights.

Cybersecurity Public-Private Partnerships in Action[18]

FBI Director Wray's remarks as prepared for delivery:

When Kaseya realized some of their customers' networks were infected with ransomware, they immediately took action. They worked to make sure both their own customers—managed service providers—and those MSPs' customers downstream, quickly disabled Kaseya's software on their systems.

They also engaged with us, early. The FBI coordinated with a host of key partners—including CISA, and foreign law enforcement and intelligence services—Kaseya could benefit from all of our expertise, authorities and reach as it worked to put out the fire.

Kaseya's swift response allowed the FBI and our partners to quickly figure out which of its customers were hit. And for us to quickly share with Kaseya and its customers information about what the adversaries were doing, what to look for and how the companies could best address the danger. Here, we were able to obtain a usable decryption key that allowed us to generate a capability to unlock Kaseya customers' data.

We immediately strategized with our interagency partners and reached a carefully considered decision about how to help the most companies possible, both by providing the key, and

by maximizing our government's impact on our adversaries, who continued to mount new attacks. Ultimately, we were able both to unlock encrypted data and to take bad actors out of operation, including by hitting Sodinokibi more broadly.

What's more, a possible conflict exists between the SEC's proposed amendments and the Federal Communication Commission's (FCC's) Customer Proprietary Network Information (CPNI) rules. The CPNI rules require telecommunications carriers to report on CPNI breaches to the Secret Service and the FBI within 7 business. However, carriers are prohibited from disclosing breaches to customers or the public for 7 days after notifying law enforcement agencies.[19]

Even the Department of Health and Human Services Office of Civil Rights offers a reporting delay under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) if a law enforcement official indicates that a notification, notice, or posting required under HIPAA would impede a criminal investigation or result in harm to national security.[20] Failure to recognize a delay for notification by law enforcement would undermine HIPAA and perhaps elevate risks to the registrant, its industry sector, affected individuals, state and/or federal investigations, and national security. Therefore, the SEC should allow for delays as outlined under HIPAA for any entities regulated by HIPAA or any other federal regulation that affords similar delays.

In addition, the Chamber supports a reporting regime that allows a reporting delay if contractual obligations would require informing another party of the notification to the government and law enforcement deems that informing the other party is undesirable or inadvisable based on the circumstances of the investigation.[21]

4.2 Disclosure of 'Aggregate' Cybersecurity Incidents: The Feasibility and Value of Such Reporting Call for Scrutiny

The proposed addition of Item 106(d)(2) would require a company to disclosure when a "series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate" (FR16599). The SEC says that registrants would be required to "analyze related cybersecurity incidents for materiality, both individually and in the aggregate." The Commission would require registrants to disclose the following elements if incidents become material in the aggregate:

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

Despite the elements listed directly above, it is unclear what events would constitute a "series of previously undisclosed" cybersecurity incidents. For example, if similar types of attacks are conducted against the same company by different actors over the course of a year

or even a longer period, it is unclear whether they would be considered a series of reportable cybersecurity incidents.

Only in hindsight—and with the contributions of industry and government cybersecurity specialists—can some hacking groups (e.g., Fancy Bear and Cozy Bear, both of which are linked to Russian intelligence) be readily considered a group of cybersecurity incidents or a relatively discernable campaign. Most often, potential material incidents in the aggregate would be difficult to identify and operationally challenging to track. In addition, the Commission's proposed definition of cybersecurity incident refers to "any information" on a company's system, so the SEC's mandate would require reviewing virtually unlimited amounts of data over indefinite periods of time.

The SEC underestimates the burdens related to tracking "several small but continuous cyberattacks against a company," which may or may not prove to be material. And the feasibility and value of such reporting to investors is questionable. The Commission should provide additional clarity around what constitutes this requirement to limit information overload to investors, particularly around events that have already occurred and been resolved by a company.

5. Streamlining Reporting Regulations Needs Greater Urgency

The Commission notes that many states have laws that allow companies to delay providing public notice about a data breach incident or notifying certain constituencies of such an incident if law enforcement determines that notification will impede a civil or criminal investigation. "A registrant may have obligations to report incidents at the state or federal level." Nevertheless, these obligations are "distinct," the SEC says, from a company's obligations to disclose material information to its shareholders under federal securities laws. In short, the SEC says that "there is a possibility a registrant would be required to disclose [an] incident on Form 8-K even though it could delay incident reporting under a particular state law." But states give companies some 30 days to notify impacted consumers. Surely, the SEC is not suggesting that investors have a greater or better interest in disclosure than the impacted consumers. The Commission should be careful to not place an emphasis on the interests of investors over impacted consumers and national cybersecurity concerns.

The proposed amendments would add yet another requirement to many companies' thick portfolio of state, federal, and in several cases international reporting mandates. SEC actions would further complicate businesses' ability to fend off illicit hacking efforts while attempting to comply with cybersecurity regulations. Some organizations may be able these additional mandates as part of an already complicated regulatory regime, but others may not, resulting in greater harm to investors.

Attending to duplicative and potentially conflicting cybersecurity regulations places a major strain on companies' limited resources, which the Commission seems to minimize as a concern. While companies must comply with many data breach disclosure requirements, the proposed rules would add another layer of complexity. The SEC says that that the requirements "may cover some of the material incidents that companies would need to report

under the [SEC's] proposed amendments, but not all incidents." The Commission notes that "the timeliness and public reporting requirements of these [other] requirements vary, making it difficult for investors and other market participants to be alerted to the breaches, and to be provided with an adequate understanding of the impact of such incidents to registrants."

Adding more government cybersecurity disclosure requirements to companies' legal obligations would not enhance U.S. cybersecurity. Indeed, the Chamber urges the SEC and other policymaking bodies to collaborate with industry to streamline the nearly countless data breach/data security/cybersecurity notification, disclosure, or incident reporting regulation, and not add to them. Where a federal regulation exists, the Chamber urges the SEC to reconsider its position on exemptions and incorporate into its proposed rule an exemption for entities that are subject to and in compliance with similar federal cybersecurity reporting regulations.

For many years, the Chamber has pressed federal policy officials to harmonize duplicative and overly burdensome information security requirements that impact regulated institutions. The SEC should not finalize its cybersecurity rules unless it can articulate a sensible plan to harmonize the multiple regulations that affect industry at the state, federal, and international levels vis-à-vis its rulemaking.

CIRCIA, or the cyber incident reporting law, calls on the NCD to lead an intergovernmental Cyber Incident Reporting Council composed of the Office of Management and Budget, CISA, and sector risk management agencies "to coordinate, deconflict, and harmonize" federal incident reporting requirements, including those issued through regulations. The law also tasks the NCD and other federal agency officials to periodically review existing reporting requirements to avoid conflicting, duplicative, or burdensome requirements and streamline those reporting requirements and submit a report to Congress.[22]

Moreover, the NCD's October 2021 strategic statement places much emphasis on cybersecurity "responsibilities to be more equitably and proportionally shared by those able to shoulder them." The NCD goes on to say, "Achieving this vision will require *cooperation* across the many public, private, and international stakeholders in the ecosystem, and it will require *coordination*, so that these efforts are not operating at cross purposes but are instead mutually reinforcing. … First, and above all else, the [NCD] will champion federal coherence across U.S. government in cyber policy, action, and doctrine. It will improve public-private collaboration to tackle cyber challenges across sectoral lines [italics in the original]."[23]

The Chamber agrees with the NCD's thinking regarding cybersecurity cooperation and coordination, which the SEC's proposed rules do not take into consideration. In the coming months, policy leaders' ability to work effectively with industry to streamline various federal reporting/disclosure/notification laws and requirements will be significantly tested. The Chamber wants to contribute to this effort.

In sum, the Chamber respects the SEC's obligations to protect investors, advocate for competition among companies, and advance capital formation. Yet its proposed cybersecurity regime overreaches by casting an overly broad net for company data. The day-to-day realities

of cybersecurity should inform the SEC that increased cybersecurity incident disclosures would probably translate into heightened risks for companies and their investors—which is the exact opposite of the Commission's policy objectives.

Without substantive changes, the SEC's proposed rules could jeopardize companies' security and resilience. The Commission needs to incorporate feedback from industry and government cybersecurity experts. It does not seem that the SEC consulted law enforcement and national security agencies in developing its rule. In a nutshell, the SEC's intended amendments fall short of both safeguarding companies and advocating for investors by:

- Elevating threats to companies' cybersecurity by compelling them to disclose more detailed cybersecurity incident data to the public, which includes criminals and other malicious actors.

- Pushing companies to potentially report too often and too early—particularly before investigations, including with law enforcement, are done—which could tip off illicit hackers and lead to inadvertent disclosure inaccuracies and negative market volatility.

- Disregarding laws and regulations that require protecting—not openly divulging—cybersecurity and related critical infrastructure information from bad actors. The SEC's rules would essentially override these policies, which have been carefully developed by government and business officials over a decade and more.

6. The Commission Should Advocate for Legal Liability Protections Tied to Material Cybersecurity Incident Disclosures

The Chamber is generally supportive of reasonable cybersecurity disclosure policies. However, existing law and regulation do not endorse the public airing of unmitigated cybersecurity incident and vulnerability information. The Chamber has significant concerns with policies that would reveal the details of a company's cybersecurity incidents to the public—including investors as well as bad actors ranging from criminal gangs to foreign powers. The 3 laws noted in this letter were written to ensure that industry reporting on significant cybersecurity incidents get shared with government (principally CISA) in a timely fashion and handled in a manner that safeguards the victim and the sensitive details of a cybersecurity incident.

The Chamber appreciates the SEC's interest in having companies make "consistent, comparable, and decision-useful disclosures." But industry is concerned with the Commission determining—without substantial justification and contrary to the judgment of Congress—what an "adequate understanding" of a material cybersecurity incident means and then having companies divulge such sensitive data to the public. The Chamber strongly believes that the details surrounding a cybersecurity incident should be handled with care and not exposed publicly until the danger that such an incident poses to the company or perhaps others is mitigated, thus denying malicious hackers the ability to exploit the incident to attack the company or similarly situated entities.

The proposed rules illustrate how fragmented policy approaches to industry disclosure can prove duplicative, confuse security requirements, and splinter organizations' risk management budgets, and cause market distortions that weaken security for individual companies and collectively. The Chamber believes that the path forward is relatively straightforward—but not easy. Congress should pass legislation that extends legal liability protections to industry for company information that is disclosed to the public because of the Commission's proposed amendments. Such a law would have the virtues of giving policymakers, the business community, and investors more of what they need.[24]

The SEC is seeking consistent, useful, and timely company disclosures on registrants' material cybersecurity incidents and security programs, which can help advise investors. Industry seeks these outcomes too. However, registrants need policymakers to better balance federal regulation with legal liability and related protections, consider the growing private sector costs of defending against nation states, and harmonize and promote U.S. policies at home and internationally. Last year the Chamber worked closely with House and Senate lawmakers on CIRCIA. The law contains both reporting requirements *and* protections that were thoughtfully negotiated by lawmakers and industry.

7. Disclosure of a Company's Cybersecurity Programs: Informing Investors and Protecting Company Data Should Be Complementary

7.1 Risk Management and Strategy

Under the Commission's proposal, Item 106(b) would require registrants to disclose their policies and procedures to "identify and manage cybersecurity risks and threats" (e.g., operational risk, intellectual property theft, and fraud).[25] Specifically, proposed Item 106(b) of Regulation S-K would require disclosure of whether:

- A company has a cybersecurity risk assessment program and a description of it.
- A company engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program.
- A company has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider (e.g., providers that have access to the company's customer and employee data).
- Cybersecurity considerations affect the selection and oversight of third-party providers (e.g., through contracts and other mechanisms) a company uses to mitigate cybersecurity risks related to these providers.
- A company undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents.
- A company has business continuity, contingency, and recovery plans in the event of a cybersecurity incident.

- Previous cybersecurity incidents have informed changes in a company's governance, policies and procedures, or technologies.

- Cybersecurity-related risk and incidents have affected or are reasonably likely to affect a company's results of operations or financial condition and if so, how.

- Cybersecurity risks are considered as part of a company's business strategy, financial planning, and capital allocation and if so, how.

The SEC states, "[M]ost of the registrants that disclosed a cybersecurity incident in 2021 did not describe their cybersecurity risk oversight and related policies and procedures." Some companies, the Commission notes, provided only general disclosures, such as a reference to cybersecurity as one of the risks overseen by the board or a board committee. The Commission is proposing Item 106(b) of Regulation S-K to require registrants to provide "more consistent and detailed disclosure regarding their cybersecurity risk management and strategy." The Commission contends that disclosure of a company's relevant policies and procedures would benefit investors by providing greater transparency regarding the company's cybersecurity risk management strategy.

The Chamber asserts that there is a reasonable explanation for why a company may provide a comparatively high-level summary rather than a detailed description of its cybersecurity risk management program. Put simply, this approach is necessary to reduce the risk of compromise from a cyberattack that could be facilitated by an adversary obtaining access to a company's relevant cybersecurity policies and procedures because of the SEC's proposed reporting regime. If the Commission moves forward with the proposal, it must take these consequences into account and thoroughly explain any analysis that justifies more detailed disclosures.

The Commission has not offered a persuasive argument that there is an unmet demand for greater transparency into a company's cybersecurity risk management efforts. Even if the SEC were to make a convincing case for increased transparency, public policy would need to be tempered to safeguard companies' cybersecurity programs. No organization—public or private—is typically willing to reveal the contents of its cybersecurity gameplan to friendly parties, much less to nation state hackers or their surrogates, which would have access cybersecurity risk oversight and related policies and procedures.

To be sure, the SEC's 2018 interpretive guidance notes that the "guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to penetrate a company's security protections." The Commission adds that it does "not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident" (FR8169).

In contrast, the Commission clearly wants companies to disclose more details in their disclosures, which is a departure from its 2018 interpretive guidance. This guidance rejects having companies "publicly disclose specific, technical information about their cybersecurity systems." But in its current rulemaking, the SEC clearly wants companies to disclose more detail in their disclosures (FR16594). The Commission should be mindful of what it requests registrants to disclose under its proposed rules. The SEC may believe that changes to its disclosure rules wouldn't put companies at a heightened risk for additional cyberattacks. However, many security specialists in the business community are alarmed by the rule and industry concerns must be considered. Information that the Commission requires to be publicly disclosed would be made available to both benign actors and nefarious hackers.

7.1.1 What Is Too Much Cybersecurity Information for Bad Actors

How much information about a company's cybersecurity risk oversight and related policies and procedures would be too risky to be made public? The SEC's rulemaking does not grapple with this important question in a way that is beneficial to companies, based on feedback that the Chamber has received. It may be useful to move from the abstract rulemaking to real-world tools and regulations, such as the joint industry and National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the Transportation Security Administration (TSA) security directive, respectively, to answer the question.

Many private entities use the popular CSF. The CSF is built on five key functions—Identify, Protect, Detect, Respond, and Recover—that provide a comprehensive view of the life cycle for managing cybersecurity risks and threats over time. The table that follows captures the 5 functions of the CSF, some basic activities under each one, and some questions that the SEC should address as is considers its rulemaking.[26]

[Go to the next page.]

7.1.2 Excerpts from NIST Publication *Getting Started With the NIST Cybersecurity Framework*: Even Basic Program Information Can Unintentionally Assist Malicious Hackers

CSF Functions	Sample Function Activities	Questions to the SEC
IDENTIFY Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	• **Identify critical enterprise processes and assets**—Describes an enterprise's activities that must continue to be viable. This could be maintaining a website to retrieve payments, protecting customer/patient information securely, or ensuring that the information an enterprise collects remains accessible and accurate. • **Maintain hardware and software inventory**—It's important to understand computers and software in an enterprise because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet.	The SEC wants more transparency into a company's cybersecurity program. But why, for example, would the Commission want to force a company to reveal its critical enterprise processes and assets to both investors and bad actors? The SEC's rulemaking is written in a way that doesn't rule out such an outcome.
PROTECT Develop and implement the appropriate safeguards to ensure delivery of services.	• **Conduct regular backups**—Many operating systems have built-in backup capabilities; software and cloud solutions are also available that can automate the backup process. • **Protect your devices**—Consider installing host-based firewalls and other protections such as endpoint security products. Apply uniform configurations to devices and control changes to device configurations.	The Protect function covers an array of technical activities to limit or contain the impact of potential cybersecurity events, which could feasibly include a material incident. These actions range from safeguarding credentials to managing data security and industrial control systems to monitoring log records. The Commission believes that the disclosure of a company's relevant

		policies and procedures would benefit investors. Yet the SEC's proposed disclosure mandates could quickly become unwise if a company's protective cybersecurity activities are revealed to illicit actors. How would the SEC balance the details that it seeks to provide investors without arming nation state hackers and their surrogates? It is unclear.
DETECT Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	• **Test and update detection processes—**Develop and test processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity. • **Maintain and monitor logs—** Logs are crucial to identify anomalies in an enterprise's computers and applications. Logs record events such as changes to systems or accounts as well as the initiation of communication channels.	The SEC's proposal would push companies to disclose whether they take actions to prevent, detect, and minimize effects of cybersecurity incidents. This line of inquiry would be understandable if responses were limited to review by investors—but bad actors would also get access. Why would the Commission ostensibly want data on a company's efforts to detect unauthorized entities on its information systems? The rulemaking does not appear to eliminate such a disclosure.
RESPOND Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	• **Ensure response plans are tested—**It's important to test response plans to make sure each person knows his or her responsibilities in executing the plan. This includes knowing any legal reporting requirements or required information sharing. • **Coordinate with internal and external stakeholders—**It's important to ensure that an enterprise's response plans and updates include all key stakeholders and external service providers. They can contribute to improvements in planning and execution.	The Respond function enables a company to contain the effects of a potential cybersecurity incident. What amount of novel detail would the Commission want a company to reveal regarding its response planning and communications with internal and external stakeholders (e.g., the FBI or the Secret Service)? Making too much detail available to investors—as well as malicious actors—could prove counterproductive to a company's security and financial performance.
RECOVER Develop and implement the appropriate activities to maintain plans for resilience and to restore	• **Communicate with internal and external stakeholders—**Part of recovery depends upon effective communication. An organization's	The SEC's rulemaking calls for a company to disclose whether it has business continuity, contingency,

any capabilities or services that were impaired due to a cybersecurity event.	recovery plans need to carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need but no inappropriate information is shared. • **Ensure recovery plans are updated—**As with response plans, testing execution will improve employee and partner awareness and highlight areas for improvement. Be sure to update Recovery plans with lessons learned.	and recovery plans in the event of a cybersecurity incident. This requirement tracks with the CSF's Recover function. The Commission's 2018 interpretive guidance insists that a company would not need to make detailed disclosures that could compromise its cybersecurity efforts. Thus, what level of detail does the SEC newly want from a company regarding its business continuity and recovery plans that is doesn't already disclose?

If, having read the table's contents, the Commission responds that it does not want companies to disclose as much detail as what is provided here, then many in industry reasonably want to know what the Commission wants from registrants that is *substantively different* from what the SEC's 2018 interpretive guidance calls for. Nevertheless, if the SEC wants a company to provide even more granularity in reports than what the table illustrates, then this level of detail into a company's cybersecurity program would be troubling. No evidence has been put forward by the Commission that such a level of detail would benefit investors or that the benefits would outweigh the potential consequences to companies that are already victims of cybercriminals or nation state actors or their surrogates.

Moreover, there is a discrepancy between the Commission's push for greater company transparency and other federal policymakers' stances on protecting government and/or industry cybersecurity programs and activities against cyber intrusions. For example, in July 2021, the Department of Homeland Security (DHS) Transportation Security Administration (TSA) issued a second security directive (the first one being issued in May 2021) requiring owners and operators of TSA-designated critical pipelines to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, among other measures.[27]

The security directive is considered sensitive security information (SSI), meaning that its disclosure would be "detrimental to the security of transportation," according to the TSA. The directive's cover memorandum warns recipients to "take special care to safeguard SSI from unauthorized disclosure and limit disclosure to covered persons … to whom access is operationally necessary."[28] Additional examples of DHS-administered regulations that mandate the protection of cybersecurity-related information are the Chemical Facilities Anti-Terrorism Standards (CFATS) program and the Maritime Transportation Security Act (MTSA). CFATS information is safeguarded as Protected Critical Infrastructure Information, and MTSA information is safeguarded as SSI.[29]

The SEC's proposed amendments are clearly at odds with the determination of DHS that information about cybersecurity incidents must be kept confidential and not publicly

disclosed. It is unclear how the SEC's rulemaking would interact with the TSA's security directives and how a company that is also subject to the TSA directive would choose which government regulation to follow.

Posting greater details about a company's relevant cybersecurity policies and procedures on a public internet website is a step that the Commission should not take. Forcing companies to make public sensitive elements about their cybersecurity risk management programs is dangerous, while the benefit to investors is uncertain. The SEC has an obligation to consider both this risk and less costly alternatives for protecting investors.

Public disclosure on whether and how cybersecurity considerations affect registrants' selection and oversight of third parties should only be provided at a very high level. Detailed information could have detrimental security implications (e.g., providing a roadmap to vulnerabilities and widespread breaches if malicious actors were to detect certain patterns). Public disclosure should be limited to confirmation that policies and procedures are appropriately applied to third-party selection and ongoing oversight as part of a risk-based framework covering the relationship life cycle.

Public disclosure should not require detailing the mechanisms, controls, and contractual details used to reduce cybersecurity risks related to providers. Otherwise, doing so could expose a company, its clients, and its employees to additional risk, which is the opposite of what the SEC is seeking in its proposed rules. Further, exposing detailed information could put a company at a competitive disadvantage if its outsourcing policies, procedures, and service provider list is openly disclosed, including being made available to competitors.

7.1.3 Security Concerns Associated With the Public Disclosure of Companies' Cybersecurity Plans Would Likely Outweigh the Potential Benefits

Energy sector stakeholders, principally the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC), have thoughtfully wrestled with questions like 21 and 22. Portions of a 2020 FERC-NERC white paper are worth capturing at length because they wrestle with the costs and benefits of public disclosures in the context of cybersecurity. The SEC may find the authors' conclusions valuable as it weighs next steps on the proposed cybersecurity rules.

FERC and NERC concluded, "Even weighing the assumed benefits of public disclosure articulated by commenters, the principal policy reason for such disclosure—incenting compliance with the CIP [short for Critical Infrastructure Protection] Reliability Standards—is *not compelling* because section 215 of the FPA relies primarily on the prospect of substantial penalties to incentivize compliance with NERC Reliability Standards, rather than through public scrutiny" [italics added].

In a related fashion, the SEC already has tools to address the shortcomings of companies' cybersecurity disclosures and enforce against investors who act on insider information. The Commission does not need to expand its reach into companies'

cybersecurity activities and governance strategies. Companies are already obligated to disclose material cybersecurity incidents in periodic reports to the SEC. Also, many policymakers and agencies believe that safeguarding private entities' security information outweighs putting such data in the hands of illicit individuals and organizations.

FERC and NERC, *Second Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards (CIP)*
September 2020 (Selected Excepts)[30]

This Second Joint White Paper was prepared by the staffs of the [FERC] and NERC following a review of the comments [to the first white paper, which was issued in 2019]. In view of the tangible risks of publishing CIP violator names and other information found in CIP Reliability Standards noncompliance submissions, the First Joint White Paper proposal is insufficient to protect the security of the Bulk-Power System and does not implement [NERC's] full legal authority to shield such information from public disclosure. Accordingly, going forward, CIP noncompliance filings and submittals by NERC will request that the entire filing or submittal be treated as [Critical Energy/Electric Infrastructure Information, or CEII] and [NERC] staff will designate such filings and submittals as CEII in their entirety. Additionally, because of the risk associated with the disclosure of CIP noncompliance information, NERC will no longer publicly post redacted versions of the CIP noncompliance filings and submittals. ...

The First Joint White Paper acknowledged that the public identification of CIP violators may result in increased hacker activity, such as scanning of cyber systems and possible phishing attempts. However, the First Joint White Paper expressed the belief that the limited information provided in the proposed cover letter would not provide an adversary with enough information to stage a focused attack on a violator's cyber assets. ...

While some commenters assert that releasing the information proposed in the First Joint White Paper would not supply an attacker with actionable information, these commenters do not address the concern that CIP information, when combined with other publicly available information, may help an attacker. Indeed, commenters supporting greater disclosure assert that bad actors may already know much of the information that would be non-public under the First Joint White Paper proposal. That certain sensitive information regarding the security of the Bulk-Power system could be available to bad actors is not a reason for greater disclosure; indeed, greater disclosure could create a forum for bad actors to aggregate and analyze data related to cyber system weaknesses.

While the First Joint White Paper framed the initial proposal as a way of balancing security and transparency concerns ... any treatment of CIP noncompliance must be consistent with the [FERC's] obligation to protect the security of the Bulk-Power System, notwithstanding the putative benefits of public disclosure raised in the comments.

Even weighing the assumed benefits of public disclosure articulated by commenters, the principal policy reason for such disclosure—incenting compliance with the CIP Reliability Standards—is not compelling because section 215 of the FPA relies primarily on the prospect of substantial penalties to incentivize compliance with NERC Reliability Standards, rather than through public scrutiny. Registered entities face considerable penalties and required mitigation activities to address noncompliance with the CIP Reliability Standards. ... After NERC submits a CIP noncompliance filing or submittal for [FERC] review, only the [FERC] may initiate a review either on its own motion or by application of the violator; third parties are not permitted to intervene or seek review of CIP noncompliance filings and submittals. Since the public does not have a statutory role

in the enforcement of Reliability Standards, public disclosure of CIP noncompliance information does not serve any statutory purpose. Although [FERC] and NERC staffs recognize the potential deterrent effect of publicizing the identity of violators in general, the security concerns discussed here outweigh the potential benefit.

8. Governance and Board Cybersecurity 'Expertise': Businesses Should Prioritize Cyber Risk Management But Not Through SEC Mandates

8.1 Governance

Item 106(c) of the SEC's proposed cybersecurity rules would require disclosure of a company's cybersecurity governance, including "the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks."[31] The Commission wants insights into the expertise of a company's management and its role in implementing the company's cybersecurity policies, procedures, and strategies. Disclosure under Item 106(c)(1) would involve the following with respect to a board's oversight of cybersecurity risk:

- Whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks.
- The processes by which the board is informed about cybersecurity risks as well as the frequency of its discussions on this topic.
- Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

According to the Commission, the proposed Item 106(c)(1) would reinforce the 2018 interpretive guidance, which states that the board's role in overseeing cybersecurity risks should be disclosed if "cybersecurity risks are material to a company's business" and that such disclosures should address how a board "engages with management on cybersecurity issues" and "discharg[es] its [cybersecurity] risk oversight responsibility."

In addition, the SEC says that proposed Item 106(c)(2) would "require a description of management's role in assessing and managing cybersecurity-related risks and in implementing a company's cybersecurity policies, procedures, and strategies." Such a description should include the following information:

- Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk—specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents—and the relevant expertise of such persons or members.

- Whether a company has a designated chief information security officer or a comparable position within the company and his or her relevant expertise.

- The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents.

- Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

8.1.1 SEC Micromanagement of Companies' Cybersecurity Governance Would Not Advance Investors Interests

The Commission ensures that companies offering securities for sale to the public must tell the truth about their business, the securities they are selling, and the risks involved in investing in those securities. Those who sell and trade securities—brokers, dealers, and exchanges—must treat investors fairly and honestly.[32] The SEC has broad regulatory authority over significant parts of the securities industry, although its authority is not unlimited.[33] The Commission regulates public companies' disclosures—not their activities. Its proposed rules are expressed in regular disclosure language. In practice, however, the rules would push companies in targeted directions regarding the development and execution of their cybersecurity policies, processes, and board composition.

According to some government officials and industry professionals, the proposed rule's governance disclosure requirements "embody an unprecedented micromanagement" by the SEC pertaining to the composition and functioning of both the management and the boards of companies. The proposal would require companies to disclose whether they have a chief information security officer (CISO), his or her relevant expertise, and where the CISO fits in the entity's organization. The proposal would also require granular disclosures about the interactions of management and the board on cybersecurity, including the frequency with which the board and management consider cybersecurity risk and related topics.[34]

It is hard to avoid the conclusion that the Commission is trying to stipulate that companies take specific cybersecurity actions. The SEC should not use its disclosure rules to prescriptively influence company activity in this regard; nor should it overstep its disclosure authority. The Commission would be granting itself additional authority to push companies on how they should operate their cybersecurity programs. The Commission should not require disclosures designed to unduly influence company behavior where it does not have such expertise.

The Chamber has been promoting sound cyber risk management practices domestically and overseas for more than a decade. Despite high-profile cyberattacks on public and private entities, we have seen a surge of business and government investments and innovations in the field of cybersecurity. Companies, not government, are the main force driving the protection and resilience of U.S. networks and information systems. In our experience, companies are increasingly integrating cybersecurity risk management practices into their corporate cultures. The Chamber wants to see this trend continue. We also want companies and agencies to work together in cyber risk management, not function as adversaries.

The Chamber appreciates the Commission's interest with respect to improving U.S. cybersecurity, but the SEC does not have the optimal homeland security, law enforcement,

intelligence, ad national security expertise to play such a role. Many companies are already regulated regarding cybersecurity—quite heavily in many instances—and U.S. government officials are working with companies literally every minute to defend online assets and information.[35] The SEC must concede that it is more than a simple pass-through for informing investors. As such, the nature of the agency's cybersecurity expertise matters. Instead of taking a regulatory jump, the SEC should work more holistically with other federal agencies that are deeply engaged in cybersecurity matters and partner with companies to craft cybersecurity policies, including ones related to disclosing significant incidents.

8.2 Board Cybersecurity 'Expertise'

The SEC proposes to amend Item 407 of Regulation S-K by adding paragraph (j) to require disclosure about the cybersecurity expertise of members of the board of directors of the registrant. The Commission's proposed rulemaking says, "If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s) and provide such detail as necessary to fully describe the nature of the expertise."

The Commission's intended requirements would "build upon the existing disclosure requirements in Item 401(e) of Regulation S-K (business experience of directors) and Item 407(h) of Regulation S-K (board risk oversight)." The proposed Item 407(j) disclosure would be required in a company's proxy or information statement when action is to be taken with respect to the election of directors and in its Form 10-K.

8.2.1 Cybersecurity 'Expertise' Is Scarce

Further, proposed Item 407(j) would not define what constitutes "cybersecurity expertise," given that such expertise could cover different experiences, skills, and tasks. Proposed Item 407(j)(1)(ii) would, however, include the following nonexclusive list of criteria that a registrant should consider in reaching a determination on whether a director has expertise in cybersecurity:

- Whether the director has prior work experience in cybersecurity (e.g., prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner).

- If the director has obtained a certification or degree in cybersecurity.

- Whether the director has knowledge, skills, or other background in cybersecurity (e.g., in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning).

Under the SEC's rulemaking, proposed Item 407(j)(2) would say that "a person who is determined to have expertise in cybersecurity would not be deemed an expert" under section 11 of the Securities Act. This proposed safe harbor is intended to clarify that "Item 407(j)

would not impose any duties, obligations, or liability that are greater than the duties, obligations, and liability imposed" on a member of the board of directors. The Commission notes that this provision should help alleviate potential concerns of cybersecurity experts who may be considering board service. The SEC adds that it does not intend for the identification of a cybersecurity expert on the board to decrease the duties and obligations or liability of other board members.

The Chamber welcomes constructive discussions with the Commission on ways to help strengthen the cybersecurity of the business community. We urge private entities, including publicly traded companies, to proactively prioritize cyber risk management activities. However, the Chamber has concerns with the SEC's call for companies to disclose the name of any board member who has cybersecurity "expertise."

First, board experts should not proliferate via implicit or explicit government directives. From an industry standpoint, the Chamber does not believe that the SEC should give itself the power to dictate or suggest which experts sit on companies' governing bodies. This type of broad mandate could easily lead to unwieldy and unintended outcomes and impact other categories of Commission-suggested board expertise.

Second, cybersecurity talent is scare globally. From a personnel standpoint, it's unclear where companies would get the so-called cybersecurity expertise that the proposed regulation would mandate. There is a well-documented lack of cybersecurity talent for the public and private sectors that would unquestionably affect companies' recruitment of board cybersecurity experts.[36] Quality information on this subject is available via CyberSeek, which has produced an interactive heat map with insights into the supply and demand for cybersecurity professionals in the U.S., including data on state and metropolitan areas. According to CyberSeek, there are approximately 598,000 cybersecurity job openings in the U.S. This significant number does not account for workforce shortfalls in other parts of the world.[37]

It is unlikely that even organizations such as NIST could readily pinpoint what constitutes expertise or experience in cybersecurity that would earn widespread agreement among industry professionals. Advancements in cybersecurity occur rapidly. Overseeing internal and external experts who are current in the field is arguably more valuable than directors having outdated credentials.

Furthermore, the cybersecurity field remains remarkably homogenous, especially in leadership positions. The SEC should consider that cybersecurity board expertise needs to draw from a nondiverse talent pool. There are a growing number of new rules and legislation that call on companies to disclose board diversity, have at least two diverse board members, and/or explain their lack of board diversity.[38] An unintended consequence of the SEC proposal is likely to create new barriers for underrepresented groups to move into cybersecurity leadership roles largely due to the expense of obtaining credentials and other formal certifications. The costs associated with obtaining cybersecurity-related degrees and other credentials could hinder the advancement of individuals who could otherwise rise through the ranks within the field of cybersecurity.

Third, the commission has not provided sufficient evidence that having cybersecurity "experts" on boards would increase companies' cybersecurity postures or advance the SEC's mission. Even assuming companies could obtain the relevant cybersecurity experts for board positions, as the Commission proposes, no evidence has been convincingly shown that this requirement would better inform investors or improve companies' cybersecurity. Board members, even with cybersecurity expertise, would not be responsible for day-to-day operations of a company, which is the level at which cybersecurity incidents occur—from social engineering to supply chain attacks.

Under the SEC's proposal, investors may see the inclusion of certain individuals on a company's board as an indication of a company's overall cybersecurity program maturity and as a sign that a company is more secure than another one that does not have a board member with cybersecurity expertise. Such an outcome could be misleading to investors. It could create a false sense of confidence among investors because a company without board members with cybersecurity expertise may have an extremely knowledgeable CISO and other staff who carry out day-to-day operations that defend the company's assets and customers. Meanwhile, the company with a board member with cybersecurity expertise may suffer from poor operational execution of policies and procedures.

The Chamber has a shared interest with the Commission in urging companies' governing bodies to prioritize cybersecurity throughout their organizations and with their business partners, but compelling companies to put hard-to-find cybersecurity experts on their boards, owing to their duties to disclose, is not the optimal way to facilitate this objective or achieve the SEC's policy goals.

9. Definitions: 'Cybersecurity Incident' Should Be Narrowed: Overreporting Incidents Would Not Serve Investor Interests

Proposed Item 106(a) defines the terms "cybersecurity incident," "cybersecurity threat," and "information systems" as used in proposed Item 106 and proposed Form 8-K Item 1.05 as follows:

- **Cybersecurity incident** means an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

- **Cybersecurity threat** means any potential occurrence that may result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

- **Information systems** means information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

According to the SEC, "What constitutes a 'cybersecurity incident' for purposes of our proposal should be construed broadly and may result from any one or more of the following: An accidental exposure of data, a deliberate action or activity to gain unauthorized access to systems or to steal or alter data, or other system compromises or data breaches."

The SEC's definition of a cybersecurity incident generally aligns with NIST's definition, which the Chamber looks to for technical authority (see the table below related to NIST terms). For reasons of consistency, federal agencies should avoid defining terms through their own nomenclature. Also, the Chamber believes that cybersecurity incident needs some refinements and boundaries—meaning that it shouldn't be overly elastic—or "construed broadly," according to the Commission.

The scope of the SEC's definition of a cybersecurity incident is too expansive. Instead, at the time of this writing, the Chamber believes that it should track more closely with *Presidential Policy Directive, United States Cyber Incident Coordination (PPD 41)*. Material cybersecurity disclosures should correspond to significant incidents that do actual harm. PPD 41 refers to a "significant cyber incident" as a "A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

Companies need clarity in reporting requirements, which should be targeted to well-defined and confirmed material cyber incidents. Some legislative and regulatory language that the Chamber has considered—such as "potential cyber intrusions" and incidents that could be "reasonably believed" to be reportable—are overly subjective. Material cybersecurity incidents should be attached to clear, objective criteria in any rule that the SEC—with industry input—develops. Getting the definition of a cybersecurity incident right requires more time that the SEC's comment period allows.

The definition of a cybersecurity incident should be limited to information systems or resources that are within the company's control. Reportable incidents could involve information resources "used by" the company even if they are not owned by the company. In many circumstances, it could be difficult, if not impossible, for a registrant to be reasonably able to obtain adequate information to make a materiality determination about cybersecurity incidents affecting third-party information resources.

A cybersecurity incident, specifically the use of "unauthorized" access as an element for disclosure review, is excessively broad. It is remote that unauthorized access to a company's information systems alone, without an intent to do wrong, would "[jeopardize] the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." If the Commission's rule is enacted as proposed, it would generate scenarios where nearly every potential breach (e.g., of company policies) or accidental access—regardless of an intent to do harm or any actual resulting harm—would need to be reviewed by a disclosure committee to determine materiality. Some state data breach laws and insurance data security laws provide exceptions for instances of good faith

access to or the acquisition of data, data encryption, or where a company has confirmed that data has been appropriately deleted or returned to the individual recipient.[39]

The likelihood of a disclosure in these instances could be remote, but the burdens placed on registrants to ensure compliance would be significant, perhaps outweighing the risk that a company fails to disclose a material cybersecurity incident, which is the opposite of what the Commission seeks.

Similarly, the disclosure of potential threats or attacks that are repelled would not provide value to investors and would not impact a company's financial performance. The SEC should narrow the scope of events that are cybersecurity incidents to align with the examples discussed in the rule that have an element of unlawfulness or intent to do harm to the company's information systems. A more targeted scope, such as using "unlawful access," would better identify the true threats to a company's information systems that investors should be aware of when making financial decisions.

The proposed definition of cybersecurity incident does not account for the fact that many industries are already subject to federal cybersecurity incident reporting obligations. The SEC's proposed definition of cybersecurity may be inconsistent with the definition of a "covered cybersecurity incident" in CIRCIA (see the table below related to CIRCIA definitions), which is a new law. The Chamber could cite other examples.

The main point is that the SEC's rules should give companies that have other federal cybersecurity incident reporting/disclosure/notification obligations the option to rely on the definition of a "cybersecurity incident" promulgated by those agencies in determining whether there was a "cybersecurity incident" and if determined to be material would be required to be reported pursuant to Item 1.05 of Form 8-K.

PPD 41 Definitions[40]

Cyber incident. An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Significant cyber incident. A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

***

NIST Computer Security Resource Center
Selected Terms and Definitions[41]

Cyber incident
Definition: Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.
https://csrc.nist.gov/glossary/term/cyber_incident

Cyber threat
Definitions: Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
https://csrc.nist.gov/glossary/term/cyber_threat

Cybersecurity
Definition: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
https://csrc.nist.gov/glossary/term/cybersecurity

Cybersecurity incident
Definition: A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
https://csrc.nist.gov/glossary/term/cybersecurity_incident

Information system
Definition: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
https://csrc.nist.gov/glossary/term/information_system

***

H.R. 2471, the Consolidated Appropriations Act, 2022 (P.L. 117-103)
Division Y—Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
Selected Terms and Definitions[42]

(4) **Covered cyber incident**.—The term "covered cyber incident" means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the [CISA] Director in the final rule issued pursuant to section 2242(b).

(6) **Cyber incident**.—The term "cyber incident"—
(A) has the meaning given the term "incident" in section 2209; and
(B) does not include an occurrence that imminently, but not actually, jeopardizes—
(i) information on information systems; or
(ii) information systems.

(11) **Information system**.—The term "information system"—
(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers. [p. 991]

Under CIRCIA, the final rule is required to include the "types of substantial cyber incidents that constitute covered cyber incidents," which must—

(A) at a minimum, require the occurrence of—
(i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;
(ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against
(I) an information system or network; or
(II) an operational technology system or process; or
(iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;
(B) consider—
(i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue;
(ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and
(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and
(C) exclude—
(i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and
(ii) the threat of disruption as extortion, as described in section 2240(14)(A). [p. 997]

***

Thank you for the opportunity to provide the Commission with comments on the proposed cybersecurity rules. If you have any questions or need more information, please do not hesitate to contact Tom Quaadman ([redacted]), Christopher Roberti ([redacted]), Matthew Eggers ([redacted]), or Evan Williams ([redacted]).

Sincerely,

Tom Quaadman
Executive Vice President
Center for Capital Markets Competitiveness
U.S. Chamber of Commerce

Christopher D. Roberti
Senior Vice President
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce

Matthew J. Eggers
Vice President, Cybersecurity Policy
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce

Evan Williams
Director
Center for Capital Markets Competitiveness
U.S. Chamber of Commerce

Notes

[1] The Securities and Exchange Commission (the SEC or the Commission), "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," *Federal Register* (FR), March 23, 2022. https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

"SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," March 9, 2022.
https://www.sec.gov/news/press-release/2022-39 (press release)
https://www.sec.gov/files/33-11038-fact-sheet.pdf (fact sheet)

[2] See "Gary Gensler's SEC Regulation Raceway: Even many Democrats are objecting to the agency's rapid rule-making." *The Wall Street Journal*, April 29, 2022.
https://www.wsj.com/articles/gary-genslers-regulatory-raceway-securities-and-exchange-commission-house-democrats-letter-11650489485?mod=opinion_major_pos1

[3] SEC, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," (aka 2018 interpretive guidance). FR, February 26, 2018.
https://www.govinfo.gov/content/pkg/FR-2018-02-26/pdf/2018-03858.pdf

In 2011, the SEC's Division of Corporation Finance issued interpretive guidance to provide the views of division staff concerning a registrant's (or a company's) existing disclosure obligations relating to cybersecurity risks and incidents.
https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[4] SEC 2018 interpretive guidance, p. 6.

[5] SEC Chair Gary Gensler, "Statement on Proposal for Mandatory Cybersecurity Disclosures," March 9, 2022.
https://www.sec.gov/news/statement/gensler-cybersecurity-20220309

[6] See "U.S. Secretary of Commerce Penny Pritzker Delivers Keynote Address at U.S. Chamber of Commerce's Cybersecurity Summit," September 27, 2016.
https://2014-2017.commerce.gov/news/secretary-speeches/2016/09/us-secretary-commerce-penny-pritzker-delivers-keynote-address-us.html

[7] The Cybersecurity Information Sharing Act of 2015 (see title N of P.L. 114-113), which had the support of both parties in Congress and the Obama administration, is a good example of a program that encourages businesses to defend their computer systems and share cyber threat data with government and private entities within a protective policy and legal structure.
https://www.congress.gov/bill/114th-congress/house-bill/2029

[8] https://www.uschamber.com/security/cybersecurity/us-chamber-letter-s-3045-cybersecurity-vulnerability-identification-and

[9] S. 3045, the Cybersecurity Vulnerability Identification and Notification Act of 2020, was incorporated into the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283) as § 1716.

https://www.congress.gov/bill/116th-congress/senate-bill/3045
https://www.congress.gov/bill/116th-congress/house-bill/6395

[10] https://www.congress.gov/116/crpt/srpt242/CRPT-116srpt242.pdf

[11] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which is division Y of H.R. 2471, the Consolidated Appropriations Act, 2022 (P.L. 117-103).
https://www.congress.gov/bill/117th-congress/house-bill/2471

[12] See CIRCIA at § 2245(a). It is important to distinguish vulnerability information from incident data. Vulnerabilities are found routinely and mitigated based on industry best practices and international standards for coordinated vulnerability disclosure and handling (CVD).

In general, information concerning vulnerabilities is kept in strict confidence during the CVD process until mitigations are publicly available. This is done to reduce the risk that sensitive information could be exploited by attackers to harm users and the cyber ecosystem.

The practice of maintaining vulnerability information in strict confidence is embodied in international standards for CVD (ISO/IEC 30111, 29147) and endorsed by Congress. See the IoT Cybersecurity Improvement Act of 2020 (the IoT Act) and CIRCIA at § 2245(a).

[13] This section of the Chamber's letter generally aligns with parts B and C of the SEC's proposed amendments (FR16595+).

[14] Cybersecurity and Infrastructure Security Agency (CISA), "New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks," November 16, 2021.
https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability
https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pd

[15] https://www.acq.osd.mil/cmmc

[16] Department of Justice, "Best Practices for Victim Response and Reporting of Cyber Incidents," April 2015.
https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf

[17] See 12 CFR Appendix B to Part 30(III)(A), which notes, "Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation."
https://www.law.cornell.edu/cfr/text/12/appendix-B_to_part_30

[18] Department of Justice, "Attorney General Merrick B. Garland, Deputy Attorney General Lisa O. Monaco and FBI Director Christopher Wray Deliver Remarks on Sodinokibi/REvil Ransomware Arrest," November 8, 2021
https://www.justice.gov/opa/speech/attorney-general-merrick-b-garland-deputy-attorney-general-lisa-o-monaco-and-fbi-director
https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-kaseya-ransomware-attack

[19] Federal Communication's (FCC) Chairwoman Rosenworcel issued proposed rules to eliminate the 7-day delay for notification of customers, but it remains in force. See "Chair Rosenworcel Circulates New Data Breach Reporting Requirements," January 12, 2022.
https://www.law.cornell.edu/cfr/text/47/64.2011
https://www.fcc.gov/document/chair-rosenworcel-circulates-new-data-breach-reporting-requirements

[20] 45 CFR § 164.412, law enforcement delay.
https://www.law.cornell.edu/cfr/text/45/164.412

[21] On February 7, 2022, the Chamber commented similarly to the Federal Trade Commission (FTC) on the agency's proposed amendment to the Safeguards Rule on standards for safeguarding customer information. The FTC's December 9, 2021, notice would require "financial institutions" to report any security event where the financial institutions have determined misuse of customer information has occurred or is reasonably likely and at least 1,000 consumers have been affected or may reasonably be affected.
https://www.regulations.gov/comment/FTC-2021-0071-0022

[22] See § 2246 of CIRCIA.
https://www.congress.gov/117/crec/2021/11/18/167/201/CREC-2021-11-18-senate.pdf

[23] The White House, Office of the National Cyber Director, *A Strategic Intent Statement for the Office of the National Cyber Director*, October 2021, p. 7.
https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf

[24] In December 2020, the IoT Act (P.L. 116-207) became law after some three years of development. Among other things, the law establishes minimum security requirements for IoT devices purchased by the U.S. government. However, notwithstanding industry urgings, Congress stopped short of developing a national, protective bill that addressed the underlying costs of increasing domestic policy fragmentation, which the IoT Act contributes to.
https://www.congress.gov/bill/116th-congress/house-bill/1668

[25] This section of the Chamber's letter largely tracks with part D of the SEC's proposed amendments (FR16599+).

[26] National Institute for Standards and Technology (NIST), Special Publication 1271, *Getting Started With the NIST Cybersecurity Framework*, August 2021.
https://doi.org/10.6028/NIST.SP.1271
https://www.nist.gov/cyberframework/framework

[27] Transportation Security Administration (TSA), "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," July 20, 2021.
https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators
https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

According to the TSA, Sensitive Security Information (SSI) is information that if publicly released would be detrimental to transportation security as defined by Federal regulation 49 CFR part 1520.
https://www.tsa.gov/sites/default/files/ssi_quick_reference_guide_for_dhs_employees_and_contractors.pdf

[28] "July 2021 TSA pipeline security directive," *The Washington Post*, October 3, 2021. https://www.washingtonpost.com/context/july-2021-tsa-pipeline-security-directive/33a019c5-d074-414a-993a-226ef7703962

Ido Kilovaty, "Cybersecuring the Pipeline" Lawfare, April 12, 2022. https://www.lawfareblog.com/cybersecuring-pipeline

[29] On the Chemical Facilities Anti-Terrorism Standards program, see 6 CFR part 29—protected critical infrastructure information. On the Maritime Transportation Security Act, see Coast Guard circular No. 10-4.
https://www.law.cornell.edu/cfr/text/6/part-29
https://www.chemicalsecurity.com/Assets/nvic-10-04-ssi.PDF

[30] Federal Energy Regulatory Commission and North American Electric Reliability Corporation, *Second Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards*, Docket No. AD19-18-000, September 23, 2020, pp. 2–7. https://www.ferc.gov/media/second-joint-staff-white-paper-notices-penalty-pertaining-violations-critical-infrastructure

[31] This section of the Chamber's letter corresponds with parts D2 and E of the SEC's proposal (FR16600+).

[32] https://www.investor.gov/introduction-investing/investing-basics/role-sec

[33] The Congressional Research Service (CRS), *Introduction to Financial Services: The Securities and Exchange Commission (SEC)*, January 13, 2022. https://crsreports.congress.gov/product/pdf/IF/IF11714

[34] SEC Commissioner Hester M. Peirce, "Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal." March 9, 2022. https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922

[35] For several years, the Chamber has urged agency officials and lawmakers to work to reduce duplicative and overly burdensome information security requirements that impact regulated institutions. To illustrate, a U.S. technology company executive shared with us in 2020 that his firm must comply with approximately 750 data security/cyber regulations globally. And about one-third of these mandates change at any given time, this person said. In a similar vein, the authors of the Fifth Domain make a compelling case for wisely pruning the regulatory bushes. They write:

> Although [the] Clinton, Bush, and Obama [administrations] eschewed, rejected, or declined to establish a [comprehensive] federal cybersecurity regulatory regime, there is a mountain of cybersecurity regulation created by federal agencies. Banks, nuclear power plants, self-driving cars, hospitals, insurance companies, defense contractors, passenger aircraft, chemical plants, and dozens of other private-sector entities are all subject to cybersecurity regulation by a nearly indecipherable stream of agencies including the FTC, FAA, DHS, DoD, FERC, DOE, HHS, DOT, OCC, and on and on. Variation in federal regulations should be a result of conscious policy choices, not the incremental accretion of rules written at different times with little central guidance. It is time to step back and assess which of these agencies and regulations have been effective.

Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (Penguin Press, 2019), pp. 113–114. The Chamber generally assumes that readers are familiar with the acronyms in the cited paragraph.

[36] For example, see (ISC)[2] blog, "Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022," February 15, 2017. By one estimate, the cyber workforce gap is estimated to be growing, with the projected shortage reaching 1.8 million professionals by 2022.
http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

House Homeland Security Committee Cybersecurity and Infrastructure Protection Subcommittee hearing, "Challenges of Recruiting and Retaining a Cybersecurity Workforce," September 7, 2017.
https://homeland.house.gov/hearing/challenges-recruiting-retaining-cybersecurity-workforce

[37] https://www.cyberseek.org/heatmap.html

[38] Nasdaq Stock Market LLC's proposed rule changes related to board diversity and disclosure. August 6, 2021.
https://www.sec.gov/rules/sro/nasdaq/2021/34-92590.pdf

Michael Hatcher et al., "States are Leading the Charge to Corporate Boards: Diversity!" *Harvard Law School Forum on Corporate Governance*, May 12, 2020.
https://corpgov.law.harvard.edu/2020/05/12/states-are-leading-the-charge-to-corporate-boards-diversify/

[39] See, respectively, the breach notification statutes of California, Texas, and New York State, as well as Virginia's Insurance Data Security Act.
https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82
https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.053
https://www.nysenate.gov/legislation/laws/GBS/899-AA
https://law.lis.virginia.gov/vacodefull/title38.2/chapter6/article2

[40] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[41] https://csrc.nist.gov/glossary

[42] CIRCIA, § 2240.
https://www.congress.gov/bill/117th-congress/house-bill/2471