May 9, 2022

File Number S7-09-22

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

Via e-mail to rule-comment@sec.gov

Dear Ms. Countryman:

BSA | The Software Alliance ("BSA") appreciates the opportunity to provide the below comments to the Securities and Exchange Commission's ("Commission" or "SEC") Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure ("Proposed Rule").[1] BSA is the leading advocate for the global enterprise software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, providing the products and services that power governments and businesses.[2] BSA's members offer software that generates efficiencies and promotes trust and security, including cloud computing, customer relationship management, human resources management, and identity and access management products and services. Businesses trust BSA members to securely handle their most sensitive information and to securely support their most critical business functions.

BSA supports the continued strengthening of cybersecurity practices across all sectors of the U.S. economy as well as the SEC's requirement that registrants make public material information about their enterprises, including information about material cyber incidents. BSA has consistently advocated policies that will strengthen cybersecurity, including as reflected in our BSA Cybersecurity Agenda which we released in October 2021.[3] As highlighted there, our priorities to improve cybersecurity include the creation of robust software security, cybersecurity for emerging technologies, modernization of government IT and cybersecurity, interoperable cybersecurity laws and policies across borders, and an effective cybersecurity workforce.

---

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (Mar. 23, 2022) ("Proposed Rule").

[2] BSA members include Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[3] BSA | The Software Alliance, "Strengthening Trust, Safeguarding Digital Transformation: BSA's Cybersecurity Agenda" (Oct. 12, 2021), available at https://www.bsa.org/files/policy-filings/10132021bsacybersecurityagenda.pdf.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

The Proposed Rule would add to the substantial existing web of state and federal laws related to the reporting and public disclosure of cyber incidents (including the recently passed Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA")). These state and federal laws are designed, if imperfectly, to balance the interests of all stakeholders, including in national security, consumer and investor protection, law enforcement, and cybersecurity. The Proposed Rule will alter this balance and risks causing significant unintended consequences. As discussed below, for example, the Proposed Rule could inadvertently compromise national security or law enforcement interests, result in investors receiving information about a material cyber incident before affected customers, and disclose sensitive information to the benefit of malicious actors.

BSA suggests that the SEC further consider how the Proposed Rule will interact with other cyber incident reporting and disclosure requirements, as well as industry best practices. The SEC should particularly focus on how its regulations weigh the concerns of other cybersecurity stakeholders to ensure its regulations are scoped correctly and do not undermine the SEC's ultimate goal. BSA is concerned that the Commission's current approach would have unintended consequences that would undermine both the Commission's goal of maintaining fair markets – a goal BSA supports – and simultaneously degrade a registrant's cybersecurity, a registrant's customers' cybersecurity, law enforcement investigations, national security activity, public safety, and the cybersecurity ecosystem more broadly. However, we see opportunities to achieve the SEC's goals, while minimizing these negative, unintended consequences, which we identify below.

The Commission Should Continue to Support Sound Cybersecurity Risk Management

We welcome the Commission's focus on advancing sound cybersecurity risk management. We agree that "[i]n today's digitally connected world, cybersecurity threats and incidents pose an ongoing and escalating risk to public companies, investors, and market participants,"[4] and that "[l]arge scale cybersecurity attacks can have systemic effects on the economy as a whole, including serious effects on critical infrastructure and national security."[5] Maintaining appropriate technical and administrative controls as part of a comprehensive, risk-based cybersecurity risk management program, with effective oversight, is critical to managing cybersecurity risk. Additional public transparency on these key points will both encourage sound practices and help investors make informed judgments about the effectiveness of a registrant's cybersecurity risk management program. BSA accordingly supports disclosure of limited relevant information about a registrant's cybersecurity policies and procedures and its board of directors' cybersecurity expertise[6]

However, if adopted as proposed, certain aspects of the Proposed Rule, namely the requirements related to Form 8-K disclosure, will have unintended consequences that will undermine the SEC's goals. We explain our reasoning below and suggest improvements that will achieve the Commission's goal of enhancing and standardizing public company cybersecurity disclosure.

The Commission Should Provide Tailored Exceptions To New Disclosure Deadlines

Targeted incident reporting can strengthen cybersecurity, particularly when it is part of robust, bidirectional sharing of information between the government and the private sector. For example, we worked closely with Congress and the Administration on the recently-passed Cyber Incident Reporting for Critical Infrastructure Act,[7] which established new requirements for the *confidential* reporting of incidents

[4] Proposed Rule, 87 Fed. Reg. at 16591.
[5] Proposed Rule, 87 Fed. Reg. at 16592.
[6] Proposed Rule, 87 Fed. Reg. at 16590.
[7] Pub.L. 117-103, Division Y.

and ransomware payments made by critical infrastructure entities. BSA does not support the public disclosure of vulnerability information, which is discussed further in the section below titled "The Commission Should Clarify That Any Incident Disclosure Requirement Does Not Apply To Vulnerabilities."

Our engagement included partnering with industry peers to highlight the key elements of an effective cyber incident reporting regime,[8] and working with key congressional committees throughout the legislative process to ensure that any legislation advance our shared goal of the increased security of the digital ecosystem.[9] Throughout this process, our focus was on ensuring that key government stakeholders learn about cyber incidents in a confidential manner so that they can use their authorities to protect American critical infrastructure, markets, consumers, and other national interests.

We agree with the Commission that a cybersecurity incident can be material to a registrant, and that investors should be informed of any material incident, cyber-related or otherwise. As the Commission explained in its 2018 interpretive guidance, disclosure of material incidents should be provided in a "timely fashion."[10] To make this possible, registrants should "maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity."[11] BSA supports this guidance and notes that, pursuant to the guidance, registrants are already expected to disclose material cyber incidents to investors in a timely manner.

The Proposed Rule would go further, however, by amending Form 8–K to add a new Item 1.05 requiring specific, detailed disclosure within four business days after a "registrant determines that it has experienced a material cybersecurity incident."[12] The Commission has not established a sufficient basis for proposing an inflexible deadline for reporting material cyber incidents – reporting that could harm a number of important stakeholders, including registrant's investors, cybersecurity risk management efforts, and the cybersecurity ecosystem more broadly. While there are situations in which the proposed disclosure requirements would work well, there are also situations, discussed more fully below, in which the unintended impact on registrants, investors, law enforcement, and the health and safety of US persons would outweigh any benefits.[13]

---

[8] *See Industry Coalition Proposes 'Central' Elements for Incident Reporting Legislation Aimed at Critical Infrastructure*, Inside Cybersecurity (Oct. 4, 2021), https://insidecybersecurity.com/daily-news/industry-coalition-proposes-%E2%80%98central%E2%80%99-elements-incident-reporting-legislation-aimed.

[9] *See, e.g.*, *BSA Welcomes Markup of Cyber Incident Reporting Act* (Oct. 6, 2021), https://www.bsa.org/news-events/news/bsa-welcomes-markup-of-cyber-incident-reporting-act.

[10] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8167 (Feb. 26, 2018) ("2018 Guidance").

[11] *Id.*

[12] Proposed Rule, 87 Fed. Reg. at 16595.

[13] The Commission has not adequately explained, for example, why cybersecurity should be treated differently from the many other critical issues that may rise to the level of a material event requiring disclosure, but that are not subject to specific Form 8-K disclosure requirements. For example, the Commission does not explain why product defects or recalls would not receive equivalent treatment, or why a disaster workplace safety incident is not subject to equivalent express requirements. Nor has the Commission adequately addressed the complex security issues raised by inflexible cyber incident public disclosure requirements, including risks that premature disclosure would present to national security, the safety of our Nation's critical infrastructure, the integrity of law enforcement investigations, and risks of disruption to fair, orderly, and efficient markets. Indeed, as noted above, Congress recently required confidential reporting of certain cyber incidents to the Cybersecurity and Infrastructure Security Agency ("CISA"), and, through CISA, notification to other key agencies within the Federal Government. Congress did *not* choose to impose inflexible deadlines for *public* disclosure of such incidents. The Commission

The Commission Should At Minimum Allow Reasonable Flexibility In Material Cyber Incident Disclosure To Prevent Severe Unintended Consequences

There are several categories of situations in which an inflexible disclosure rule would create significant, unintended harms. In our view, these harms can be minimized by adding a tailored, balancing test as an exception.

The Commission asked in the proposing release: "Could any of the proposed Item 1.05 disclosures or the proposed timing of the disclosures have the unintentional effect of putting registrants at additional risk of future cybersecurity incidents?"[14] The answer is unequivocally "yes," but future cybersecurity incidents are just one of risks that would be created if the Proposed Rule is adopted without the modification we propose in this section. The consequences of premature disclosure (i.e., disclosure that would not occur on a four-business-day timeline if appropriate consideration were given to the full balance of relevant interests) would, in certain instances, include:

- Substantial harm to national and homeland security, law enforcement investigations, and other aspects of the public interest:
    - Cybersecurity incidents can put national security interests at risk. For example, an attack on a defense contractor might implicate the confidentiality or integrity of systems that hold sensitive government information. Likewise, an attack on a critical infrastructure provider may lead to the loss of critical functions across a particular region within the United States. In those cases, numerous government agencies with national security and homeland security missions are likely to be heavily involved in the response to the incident. Managing the public disclosure of the incident will likely be an issue of top priority for those government agencies, as premature disclosure could cause the malicious actor to expedite or escalate its attack, lead to misinformation or panic, or have other negative consequences.
    - Law enforcement agencies investigate cyber incidents, gathering information about malicious actors so that they can bring prosecutions, use civil or criminal tools to take down botnets or other malicious systems, or take other appropriate legal action. Premature public disclosure of an incident will disrupt some ongoing investigations, depriving law enforcement agencies of the time they need to take actions that will help the American public.
    - The public itself may be harmed directly by premature disclosure of a cyber incident, (let alone information related to a vulnerability, discussed further below). Customers and other members of the public may be injured by any action that prompts a malicious actor to accelerate their attack or that encourages another malicious actor to attack the company, or another company using the same exploit. Possible examples are innumerable, including premature disclosure that triggers a malicious actor exfiltrating personal data, disabling a registrant's information systems, or otherwise attacking devices on which customers rely (e.g. connected medical devices, communications systems, etc.).
    - The public interest in information sharing also may be harmed by a regulatory requirement that mandates a specific timeframe for public disclosure of material cyber

should not impose such incident disclosure deadlines by rule here; the known risks are too great to justify any anticipated benefits.

[14] Proposed Rule, 87 Fed. Reg. at 16597.

incidents. As noted above, cybersecurity information sharing can be a valuable part of an effective national cybersecurity strategy. For example, CISA and the Federal Bureau of Investigation regularly inform companies when the agencies identify activity indicating that the company has been the victim of a cyber incident. But government agencies may determine not to share information about ongoing incidents with a victim company if those agencies know that the victim company is required to publicly disclose that valuable intelligence on a short and mandatory timeline. Additionally, companies often share valuable cyber threat indicators with the US Government pursuant to written agreements and through CISA's processes, in both cases, information is typically shared subject to defined confidentiality protections. Such sharing programs help government agencies and companies detect, protect and respond to malicious cyber activity. But the timeline for mandatory public disclosure in the proposed rule may chill this sharing as the registrant in a position to share information will be concerned about starting the clock for mandatory public disclosure.

As a result, a mandatory incident disclosure requirement is likely to degrade the necessary collaboration between private sector and government partners.

- Substantial harm to registrants:
    - Premature disclosure of an incident — particularly before a registrant has successfully responded to a malicious actor's access to its network — could cause substantial negative consequences for a registrant because it would alert the malicious actor that the registrant is aware of their malicious actions. For example, public disclosure of the incident may provoke the malicious actor to expedite its attack, such as by exfiltrating data in a manner that the registrant could have prevented if it had more time to respond to the incident. Likewise, public disclosure may provoke a malicious actor to undertake destructive attacks, such as by encrypting or destroying customer data, again in a manner that the registrant could have prevented with more time.
    - Premature disclosure of an incident likewise could cause substantial negative consequences for a registrant because it could encourage other malicious actors to attack the company or use similar exploits on other companies. If the registrant has not been able to secure its systems in time, it may be subject to multiple successful attacks, dramatically expanding the negative consequences that it may face.
- Substantial harm to investors:
    - Investors will bear the ultimate financial consequences of unnecessary losses imposed upon a registrant because of premature disclosure of a material cyber incident. While cyber incident disclosures may be intended to alert investors to material information, investors should not have any potential loss compounded by regulatory requirements that expand the cyber risks to registrants after an incident.
    - Premature disclosure of cyber incidents will disrupt the fair, orderly, and efficient operation of the market, hurting investors. Importantly, in many instances, a registrant will likely be able to determine that a cyber incident is material but not be able to discover accurate, complete, or even useful information about the material cyber incident to disclose within four days. Such disclosure, which would occur when the full consequences of the incident are unknown and before a registrant has reasonable time to respond to or recover from the material cyber incident, will result in investors making decisions based on information that almost certainly will be incomplete and will have a

significant likelihood of being inaccurate, resulting in market distortions that hurt investors.

We certainly support requirements to provide investors timely information about the cybersecurity policies of the companies in which they invest, including whether they are victims of material cyber incidents. Mere engagement with law enforcement or other government agencies about a material cyber incident does not justify delay in providing such notification to investors. Investors' loss of confidence in the company's cyber risk management also clearly would not be a sufficient basis to justify a delay in disclosure.

It is critical, however, that the SEC recognizes that in many instances a registrant will not be able to discover accurate, complete, or even useful information within four days of determining it is the victim of a material cyber incident. Therefore, if the Commission requires public disclosure of a material cyber incident on Form 8-K, it should create an exception that allows companies, under appropriate circumstances, to delay disclosure of an incident when premature disclosure can be reasonably anticipated to cause substantial negative consequences to a registrants cybersecurity, a registrant's customers' cybersecurity, law enforcement investigations, national security activity, public safety, and the cybersecurity ecosystem more broadly. Specifically, the Commission should create a new Item 1.05(c) as an exception to Item 1.05(a).[15] That new exception would read:

> *No disclosure shall be required if the registrant: (a) determines that disclosure of a material cyber incident would be reasonably anticipated to cause substantial harm to registrant's cybersecurity, the registrant's customers cybersecurity, law enforcement investigations, national security activity, public safety, or the cybersecurity ecosystem more broadly; (b) documents its reliance on this exception, including any consultation with appropriate law enforcement and government agencies, as appropriate; and (c) assesses, regularly, the applicability of this exception.*

We believe this is a reasonable approach as it would require a registrant to make a formal determination that it reasonably anticipates its disclosure of the material cyber incident would cause substantial harm. We accordingly ask the Commission to allow registrants to make such a reasoned judgment, document their determination, and regularly revisit the applicability of this exception.

The Commission Should, If It Requires Public Disclosure, Reduce the Information It Proposes Registrants Report on Form 8-K

The Commission proposes registrants report: (i) "When the incident was discovered and whether it is ongoing; (ii) A brief description of the nature and scope of the incident; (iii) Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose; (iv) The effect of the incident on the registrant's operations; and (v) Whether the registrant has remediated or is currently remediating the incident." The Commission proposed to do require these disclosures because it believes "that this information would provide timely and relevant disclosure to investors and other market participants (such as financial analysts, investment advisers, and portfolio managers) and enable them to assess the possible effects of a material cybersecurity incident on the registrant, including any long-term and short-term financial effects or operational effects."

BSA is concerned that, in some circumstances, publicly disclosing information as extensive as the SEC proposes might itself be detrimental to the registrant's cybersecurity, the registrant's customers' cybersecurity, law enforcement investigations, national security activity, public safety, and the cybersecurity ecosystem more broadly. Again, assuming that a registrant would be in a position to know

[15] A corresponding change would also need to be made to Item 1.05(a). For example, it could be revised to begin "Except as provided in section (c), if the registrant experiences . . .".

of and report any of this information within four days of determining that it was a victim of a material cyber incident, publicly disclosing this information would signal to the malicious actor that the registrant is aware of its actions, how much the registrant knows about the actions, whether the registrant believes it has effectively responded to the malicious actor or whether the registrant believes the malicious actor is still in the registrant's systems, among other things. In turn, publicly disclosing this information could provoke the malicious actor to exfiltrate data, destroy devices, or otherwise interrupt the registrant's activities because the malicious actor would know from the required public disclosure that the registrant was aware of its malicious actions. Further, four days is likely not sufficient time for a registrant to respond to an incident, for example, by backing up data. For example, backing up data may be a critical action to take in response to a cyber incident and the inability to do so before publicly disclosing a material cyber incident, could cause irreparable harm. Additionally, a registrant's public disclosure of this type of information may have negative consequences on other organizations, because if a malicious actor is informed by a publicly-filed Form 8-K that one company is aware of its actions, the malicious actor would expect that in the near future both government agencies and other companies will identify its tactics, techniques, and procedures and consequently, the malicious actor will likely expedite its activities on other networks, including destroying information and information systems. Finally, required public disclosure will also impede law enforcement investigations, which often rely on the cooperation of registrants, making it even harder for law enforcement agencies to bring malicious actors to justice.

Rather, BSA suggests that, if the SEC requires the public disclosure of a material cyber incident on Form 8-K, the SEC provide a registrant flexibility both on the timing and substance of the public disclosure. Public disclosure of information about a material cyber incident risks negatively impacting the registrant's cybersecurity, the registrant's customers' cybersecurity, law enforcement investigations, national security activity, public safety, and the cybersecurity ecosystem more broadly. However, providing a registrant temporal and substantive flexibility to report material information would allow the SEC to achieve its mission while limiting risk associated with public disclosure of information surrounding a cyber incident.

The Commission Should Clarify That Any Incident Disclosure Requirement Applies Only To Companies For Which the Cyber Incident is Material, Not Third Party Service Providers

The Commission correctly acknowledges the important role that third party service providers play for American businesses and government agencies. For example, cloud-based services, including many offered by BSA member companies, are integral and vital elements of all areas of American enterprise, from the support of corporate functions to the operation of critical infrastructure. Providers of these third-party services accordingly have extensive experience responding to incidents and notifying affected customers once the key facts are understood and actionable information can be provided. This approach is typically reflected in contract, which balance the third-party service provider's need to gather and provide meaningful information in an orderly and coordinated way with the customer's need to understand the risk and consequences of an incident in a timely manner. Under this approach, the third-party service provider evaluates and meets any disclosure or notification obligations based on the impact of the incident on the customer's specific business. For example, in the event of an incident involving a Software as a Service ("SaaS") provider, a cyber incident's impacts may be material to one customer but not to a second customer – and importantly, the SaaS provider would not have relevant information to determine if the impact of a cyber incident is material.

The Commission should support this established approach to the extent that it chooses to treat material cyber incidents differently than other material events and impose any specific cyber incident disclosure requirement by rule. To do so, the Commission should clarify that any specific cyber incident disclosure requirement applies to end-user businesses, not to third-party service providers. Any other approach could create chaos in the event of an incident involving a third-party service provider. Take the hypothetical example, flagged above, of an incident involving a SaaS provider, though note that this is

true for third-party service providers more generally. If the SaaS provider were required to publicly disclose the incident through an 8-K filing, rather than permitted to notify its customers in an orderly manner, the SaaS provider's customers would have to make their own determinations of materiality without access to sufficient information about the incident its SaaS provider disclosed. The end result could be an over-disclosure of cyber incidents, disrupting the marketplace, creating unnecessary noise that would confuse companies and investors alike and potentially companies taking costly and unnecessary prophylactic steps including stopping the use of important systems. This ambiguity would exacerbate the consequences of the incident — and without reason. Such a scenario would also amplify the potential negative consequences of a ransomware attack to which a registrant may be actively responding.

The Commission should avoid such unintended consequences by supporting the cooperative and agreed-upon approach through which third-party service providers currently report cyber incidents to their customers. This complex area is covered by contracts between a third-party service provider and its customer, and frequently the third-party service provider has no knowledge of or relationship to its customer's end user. Upsetting the current situation would greatly increase complexity and uncertainty without improving either market fairness or cybersecurity. The Commission should avoid such unintended consequences by clarifying and supporting the continued reporting of incidents by third-party service providers to their customers, consistent with contractual arrangements.

The Commission Should Clarify That Any Incident Disclosure Requirement Does Not Apply To Vulnerabilities

The Proposed Rule would define a "cybersecurity incident" as "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."[16] This definition is anchored by the concept of an "occurrence," i.e., an event that *has* occurred. We accordingly understand the Commission to intend for this provision to cover incidents as they are broadly understood within the cybersecurity community – i.e., events that impact the confidentiality, integrity, or availability of a system.[17] For example, this would typically include an attack by a malicious actor that compromises an online database, an email account, or other information system. In contrast, we understand this definition *not* to include a vulnerability that a malicious actor could attempt to exploit in a future attack, which, if successful, could become a cyber incident.

It is important to distinguish information regarding cyber "incidents" from information regarding the underlying "vulnerabilities" that a malicious actor may leverage in the incident. Vulnerabilities are found routinely and mitigated based on industry best practices and international standards for coordinated vulnerability disclosure ("CVD"). While the software industry works diligently to find and remediate vulnerabilities before they can be exploited, and customers patch their systems regularly to address identified vulnerabilities, malicious actors sometimes exploit vulnerabilities, which can lead to a material cyber incident. Generally, absent information on broad exploitation in the wild, information concerning

[16] Proposed Rule, 87 Fed. Reg. at 16619 and 16622.

[17] Other definitions in statutes and standards are in line with this understanding. *See, e.g.*, 6 U.S.C. § 659(a)(5) ("the term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;"); National Institute of Standards and Technology, Computer Security Resource Center, Glossary: Incident ("An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."), https://csrc.nist.gov/glossary/term/incident.

vulnerabilities (which do not amount to a cyber incident or material cyber incident) is kept in strict confidence, during the CVD process, until mitigations are publicly available. Both government agencies and industry keep this confidence to reduce the risk this sensitive vulnerability information will be exploited by malicious actors to harm a governments, businesses, or individuals. This practice, to maintain vulnerability information in strict confidence prior to mitigations being developed and made available is embodied in international standards for CVD, e.g. ISO/IEC 30111 and 29147. These standards were endorsed by Congress in the recently-passed Cyber Incident Reporting for Critical Infrastructure Act, Division Y, H.R. 2471 (P.L. 117-103), which directs the Director of CISA to "develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards."

This approach is the correct one and should be preserved if the Commission decides to impose specific requirements for reporting a material cyber incident by rule. Security vulnerabilities – i.e., "attribute[s] of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control"[18] – should be disclosed through companies' existing vulnerability management and disclosure programs according to industry best practices and international standards. As we have previously stated, "the guiding principle of [coordinated vulnerability disclosure] is that the public is best served when vulnerabilities are reported directly to vendors that can fix them and when public disclosures are delayed until the vendor has had an opportunity to develop, test, and deploy a patch to mitigate the underlying vulnerability."[19]

The Commission would up-end effective vulnerability disclosure programs by requiring vulnerability disclosures in the same manner as incident disclosure. Such an approach could have catastrophic security consequences: since vulnerabilities can take months to patch in some cases, premature public disclosure would alert malicious actors to the vulnerability and facilitate their attacks. As noted above, we understand the Commission not to intend to require such vulnerability disclosure under the Proposed Rule. We would ask the Commission to expressly confirm that this rule does not deviate from a registrant's requirement to report material events rather than potential events, in any final rule, however, to avoid any potential uncertainty.[20]

[18] 6 U.S.C. § 1501(17).

[19] *See* BSA, Guiding Principles for Coordinated Vulnerability Disclosure (2019), https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdf.

[20] The Commission notes in the Proposed Rule, for example, that "the 2018 Interpretive Release reminds companies, their directors, officers, and other corporate insiders of the need to comply with insider trading laws in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches." 87 Fed. Reg. at 16594. While we do not believe that the Commission intends to treat vulnerabilities in the same manner as incidents, for the avoidance of doubt, we would ask that the Commission clarify that it views vulnerabilities as a "risk," and does not view the category of incidents as including "vulnerabilities and breaches."

***

BSA is committed to working with the Commission to identify and address challenges relating to the appropriate disclosure of cybersecurity risks, incidents, expertise, and governance. We look forward to this continued collaboration.

Sincerely,

Henry Young

Director, Policy