PERKINSCOIE
COUNSEL TO GREAT COMPANIES

Updating Corporate and Cybersecurity Practices To Satisfy the SEC's Final Cybersecurity Disclosure Rules: Assessing Materiality of Cybersecurity Incidents

09.18.2023 | ARTICLES

The U.S. Securities and Exchange Commission (SEC) announced the final version of its long-anticipated cybersecurity rules on July 26, 2023. One new rule that will affect cybersecurity teams and executive management most directly requires covered companies to publicly disclose a "material" cybersecurity incident within four business days of determining that the incident is material.[1] Companies will have to comply with the rule beginning December 18, 2023.

The legal and reporting structures and requirements of the new rule are described in a separate post, and some important aspects of making materiality determinations are described here. But chief information security officers (CISOs), cybersecurity attorneys, and the executives and boards they advise require practical guidance on how to incorporate the new rule while planning for and conducting cyber incident response (IR).

Overall, the new SEC rule should be interpreted based on its purpose: to provide transparency and consistency of disclosure to investors about publicly traded companies. It is not designed to promote information sharing between companies, establish public-private partnerships, enhance law enforcement or national security efforts, mitigate cyber threats, or remediate cybersecurity incidents. The point is to inform the investing public.

Critically, complying with the new SEC rule is not simply a matter of providing sufficient information to satisfy legal requirements. Unlike most other federally mandated cybersecurity incident reporting, reports under the SEC rule must be *publicly available*. Four days after determining that an incident is material, a company must publicly describe what happened and the expected impact on the company. IR professionals are painfully aware that many aspects of an incident, including its technical and business impacts, may not be clear within such a short timeframe. As a result, while companies must make *sufficient* disclosures, they should also avoid making *excessive* disclosures or overcommitting to a conclusion. It is therefore important not only to conduct an informed materiality analysis, but also to limit the rapid, public disclosure to what the new rule requires.

Companies should distinguish between the new SEC rule and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA has different goals, contemplates a different and confidential reporting mechanism, and contains different thresholds—and has not been put into effect by regulations. The SEC may revise the new rule if a conflict with CIRCIA emerges, but CIRCIA should not currently factor into companies' reporting decisions under the SEC rule.

Quick Vocabulary

Cybersecurity practitioners applying this guidance may be unfamiliar with the SEC's reporting terminology. Particularly relevant terms include:

- **Form 8-K.** SEC form for "current reports" that reporting companies must file to announce certain types of events (which the form lists) that shareholders should know about. These reports are filed promptly, in between companies' regular reporting.
- **Item 1.05.** Type of Form 8-K that requires disclosure of material cybersecurity incident.
- **Cybersecurity incident.** An "unauthorized occurrence" or a "series of related unauthorized occurrences" conducted on or through a company's information systems that jeopardizes the confidentiality, integrity, or availability (CIA) of the company's information systems or any information they contain. "Unauthorized" can include "accidental."
- **Material.** Information is "material" if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the total mix of information made available to investors.
- **Information systems.** Electronic information resources owned or used by a company to process, maintain, use, share, disseminate, or dispose of the company's information to maintain or support company operations. Includes physical or virtual infrastructure controlled by such information resources or components thereof.[2]

The use of the term “jeopardizes” in the definition of “cybersecurity incident” caused concern among the public, but the SEC has noted that a cybersecurity incident only becomes relevant for the new rule’s purpose if it has a material impact.

When the Clock Starts

The *reporting* clock starts when a company determines that a cybersecurity incident is material, but compliance with the SEC reporting requirement really begins once the incident is discovered. The SEC will require companies to assess an incident’s materiality “without unreasonable delay” after discovery. The SEC changed this phrasing from “as soon as reasonably practicable” to avoid putting undue pressure on companies to report before they have gathered sufficient information. The SEC has made clear that “a materiality determination necessitates an informed and deliberative process” but has also made clear that companies may not delay their materiality determinations to postpone the reporting deadline. The *assessment* clock therefore has no fixed period, but companies should expect their assessment process and timeframe to be scrutinized for reasonableness. Careful recordkeeping can help demonstrate after the fact that a company acted without unreasonable delay and made its materiality determination at an appropriate time.

Because the assessment period is used to develop information that bears on materiality, it can and should be used to clarify and memorialize the categories of information that the company will have to report.

If and when the assessment yields a determination that the incident is material, the *reporting* clock starts. Companies must use Form 8-K to report within four business days of that determination.[3]

During the Assessment—Determining Materiality

The SEC explicitly declined to provide a materiality definition specific to cybersecurity events. Instead, the SEC directs companies to apply the long-standing definition of materiality that is used in securities law: information is material if **there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decisio**n or if it would have **significantly altered the total mix of information made available** to investors.

Materiality is assessed from the perspective of a **reasonable investor** based on all relevant facts and circumstances. These include both **qualitative and quantitative factors**. As a result, the nature of affected data is as important as the amount of affected data.

Determinations regarding materiality will likely include, at minimum, a company’s cybersecurity team, lawyers supporting that team, members of the C-suite, and securities attorneys. Whatever the composition of the team, it is crucial to focus on the impact of a potential cybersecurity incident on the company overall, and not to focus exclusively on “classic” cybersecurity questions.

Cybersecurity experts will have at least two roles. First, they will fulfill their familiar function of assessing the technical and direct consequences of a cybersecurity incident. That assessment alone may be sufficient to establish materiality. But their second function is to help the interdisciplinary team think more expansively about collateral ways in which the incident could materially affect the company.

For example, the SEC directs companies to consider “both the immediate fallout and any longer term effects” of an incident. Those effects include downstream effects on a company’s operations, finances, brand perception, customer relationships, and other aspects of the business that may or may not be tangible or quantifiable. Reasonably foreseeable harm that may not occur immediately, but that may develop over time, must factor into the materiality analysis—such as harm from the theft of trade secrets or an undermining of consumer trust in a company’s security.

Materiality determinations focus on the impact of an incident on the business and investors. As a result, a compromise of a third-party vendor such as a cloud service provider can constitute a material cybersecurity incident at a company if it has a sufficient effect on the company itself.

Based on the SEC’s advice, an affected company and its IR team should incorporate the following guidance when assessing materiality:

- Take a **holistic** view of materiality.
  - Do not rely exclusively on quantitative thresholds.
  - Does the type of data affected create particular risk?
  - Does the type of system affected create particular risk?
  - Does a cybersecurity event have a direct impact on operations or the value of the company?

    - Does a cybersecurity event create downstream risk to the confidentiality, integrity, or availability of customer data or systems?
    - Does that event create longer-term risk for the value of the company?
        - Impact on competitiveness based on theft of intellectual property (IP) or customer lists.
        - Loss of customer confidence in privacy of information.
        - Loss of customer confidence in security and/or continuity of operations.
        - Impact on reputation.
        - Impact on vendor relationships.
    - Does the event expose a security flaw or other information that contradicts representations the company has previously made?
        - Does the fact or nature of the compromise expose the company to potential liability for prior statements, actions, or inaction regarding security?
    - Does the event raise the likelihood of litigation, regulatory action, or investigations?
- A company can have sufficient information to determine that an incident is material **before an investigation is complete**. Possessing sufficient information makes the company responsible for making that determination promptly and starts the reporting clock.
    - A company should not wait to report until a full IR or investigation concludes if the company has sufficient information to make a materiality determination.
    - If "crown jewels" or key operational systems have been compromised, a company probably knows enough to make a materiality determination. This knowledge may well start the reporting clock even if a full investigation is not yet complete.
    - If an unauthorized actor has had access to or exfiltrated a large amount of important data, a company similarly probably has sufficient information to determine that an incident is material, and the reporting clock may start even if the full investigation is not yet complete.
    - The scenarios in the SEC release did not distinguish between encrypted and unencrypted data. Whether or not the affected data is encrypted, and whether or not an unauthorized actor possesses or obtains the key, will affect the materiality analysis but may not be dispositive.
- Although the SEC "streamlined" the substantive reporting requirements and imposed a short deadline, ensure that the report is **not misleading, including by omission**.
    - Legal and technical cybersecurity personnel in particular should probe IR teams' conclusions. For example, is a statement that a certain repository was not affected based on affirmative evidence, a lack of evidence, or inability to conduct analysis before the reporting deadline? If structured data fields were encrypted or otherwise protected, what about free text fields?
    - Identifying "known unknowns" in the initial report and filing an amended report once those gaps are filled is acceptable and contemplated by the new rule, as long as the review and determinations are not unreasonably delayed.
    - It is essential to file corrections—either of inaccurate statements or material omissions—promptly.
- When assessing whether an incident is material, following "**normal internal practices and disclosure controls and procedures** will suffice to demonstrate good faith compliance."
    - A company should not change assessment or reporting criteria during an incident response for a purpose that appears to be delaying the required report.
    - If a board committee or other group must be convened to make the determination, a company should not defer or delay the meeting beyond the time it would usually take to convene the group.
    - For third-party incidents, there is no need to gather information outside of "regular channels of communication" with the relevant third-party service provider.
- Resolve doubt as to whether information is material **in favor of disclosure**.
- If a company is aware that reportable information has not been determined or is not available by the reporting deadline, it should **identify known gaps** in the report it files with the SEC and file an amended report when it has additional information.
- Do not assume that sharing threat information with private sector or government entities implies that a company has determined an incident to be material. The SEC clearly stated that alerting other parties of a threat does not in and of itself trigger a reporting

obligation if the impact on the company is not material.

Contents of the Report

The SEC's final rule "streamlined" the disclosure requirements to focus on "an incident's basic identifying details" and its material impact (or reasonably likely material impact) on the affected company. Accordingly, a report must describe "material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."[4]

The SEC does not aim to require disclosure of details that threat actors could exploit. The new rule expressly does not contain a standalone requirement for "disclosure regarding the incident's remediation status, whether it is ongoing, and whether data were compromised." To the extent that details such as "data theft, asset loss, intellectual property loss, reputation damage, or business value loss" are material to the report, however, they must be included. A company is not required to "disclose specific or technical information about its planned response to the incident," its cybersecurity, or system vulnerabilities that would impede response or remediation.

Exceptions: Public Safety Delay, Classified Information, and Customer Proprietary Network Information

The SEC only provides a narrow basis for delaying a report beyond the four-business-day deadline. The deadline can only be extended if the U.S. Attorney General finds that a disclosure would pose a substantial risk to national security or public safety. The basis for the finding can come from a different agency, so a local law enforcement or U.S. Intelligence Community agency, for example, can ask the attorney general to make the finding, but only the attorney general can authorize a delay in reporting. This process will likely be used rarely.

SEC rules already provided for the omission of classified national security information from public reporting. That provision applies to reporting under the new rule.

Finally, if a company suffers a breach of customer proprietary network information (CPNI) that is subject to the Federal Communications Commission (FCC) requirement to notify federal law enforcement seven days before disclosing the breach publicly, the company may follow the FCC rule with written notice to the SEC.

After Filing the Report or Determining That a Report Is Not Necessary

Because of the short reporting timetable, it is possible that a company will develop additional reportable information, determine that additional information is reportable, or need to correct its report. New reportable information about an incident should be filed by amending the original report within four business days of the information becoming available or of the determination that it is reportable (presumably depending on why it was not included in the initial report). A company is not required to report *all* new information going forward; it only has to amend its original report with (1) new information that would have been called for in that original report; (2) information that has been newly determined to meet reporting requirements; (3) information correcting the original report; or (4) information addressing a material omission in the original report.

If a company investigates an event and determines that it is not a "cybersecurity event" under the SEC rule, the company may still have to report it later in time if the company determines that it is part of a "series of related unauthorized occurrences" that together have a material effect. Potential examples include small, continuous attacks from a single source or multiple attacks from multiple sources that exploit the same vulnerability. In either case, the impact of such attacks may only be material in the aggregate.

Incorporating Compliance With the SEC Rule Into IR Planning

Companies should ensure that their substantive and procedural IR planning takes the new SEC reporting rule into account.

Substance

Substantively, although the precise nature of a cybersecurity incident is impossible to predict, the interdisciplinary response team can develop factors that would help rapidly determine whether a future incident is material. A company's dependence on trade secrets, customer data, 24/7 availability of data and communications, cyber-physical controls, or logistics and inventory control, for example, is a good starting point for such analysis. Assess whether different types of compromises to different systems are likely to have a material impact on business. Existing practices of classifying information security events based on severity may be useful. So could developing a cyber "materiality matrix" that takes into account the impact of a cybersecurity incident. But the SEC is

unlikely to look favorably upon companies that rely exclusively on applications of formulas to assess materiality. Any decisional frameworks should take into account both quantitative and qualitative effects of an incident and should build in consideration of incident-specific impacts.

Companies should also examine representations they have made about the security of their systems and data, as well as their compliance with applicable regulations and industry best practices. Beyond the reputational harm and impact on consumer confidence that a cybersecurity incident can cause, could a security incident reveal inaccuracies in a company's prior public statements? Has the company made commitments to regulators, litigants, shareholders, customers, or other constituencies, whether in the United States or overseas, that a cybersecurity incident could call into question? Will scrutiny of the company's security posture reveal a deficiency that adopting best practices would have corrected earlier? How will different constituencies—consumers, shareholders, regulators, and litigants—react?

These are questions that cybersecurity or IR professionals cannot answer on their own. Executives and counsel with a broad view of the company and a nuanced understanding of materiality (and relevant case law and enforcement actions) must participate in IR planning.

Process

The need for interdisciplinary work to assess materiality raises questions of process. Given the short deadline the SEC has imposed and its warnings about undue delay, it is critical for companies to incorporate into their IR plan a workstream with deadlines to assess materiality and prepare a report if needed.

The "SEC workstream" should consist of a group that is small enough to work quickly and efficiently, but representative enough to provide the necessary interdisciplinary analysis. Most companies already have "disclosure committees" that meet to address other public disclosures the companies make in SEC filings, but a cybersecurity incident requires additional expertise that those on the disclosure committee might not have that are necessary to make the materiality determination.

The IR plan should identify core members (such as executive, legal, and cybersecurity representation) and specific points of contact from additional parts of the company who can be brought in as needed based on the nature of an incident. Assessing materiality is a legal obligation and involves legal analysis and advice, so limiting distribution and maintaining confidentiality of the workstream's deliberations will be important considerations to support any future claim of attorney privilege.

The "SEC workstream" group (including the core group and additional points of contact [POCs]) must remain engaged after the company files the initial report to address any gaps the report identified and ensure that material misstatements or omissions in the initial report are reported promptly in an amended report. Everyone involved must understand that they are both encouraged and required to flag new facts or analysis that may supplement—or even contradict—the initial report. For example, an observation stating, "We reported X based on facts available to us, but now that may not be accurate" may be one of the most important contributions a team member can make as IR efforts proceed beyond the initial reporting date. A company must subject such observations to a materiality analysis under the substantive criteria, interdisciplinary approach, and procedural timetable discussed above.

As noted above, event classification schemes and decision matrices have important roles in assessing materiality, and they should reflect input from executive, operational, legal, cybersecurity, marketing, financial, human resources, research and development, and other perspectives as appropriate to a specific company.

The SEC's inclusion of aggregated incidents within the reporting requirement presents a process challenge. Information security teams probably already triage events to determine whether they bear similarities to other events, such as tactics, malware, or vulnerabilities. Because individual events that do not trigger an all-out IR process will likely only be noticed by security personnel, they need to be made aware of the need to identify a series of related events, and they must be responsible for flagging such a series to their management. Training and periodic reminders will be critical. A company should have a process for evaluating the materiality of such a series that similarly leverages all relevant disciplines and applies the same criteria discussed above. Those with questions about how the new cybersecurity disclosure guidelines should contact experienced counsel.

Endnotes

[1] This note focuses on assessing materiality and reporting material cybersecurity incidents. It does not address whether the new SEC rule applies to a particular company and does not discuss other new SEC requirements related to cybersecurity that are not related to specific incidents.
[2] Operators of cyber-physical or other critical infrastructure should note that the SEC rule does not use the term "operational technology." We recommend reading the inclusion of infrastructure controlled by information resources in the definition of

“information systems” to incorporate operational technology. See Final Rule at 81.
[3] The SEC adopted rules that make disclosures eligible for limited safe harbor treatment under securities laws because of the rapid timeframe for making materiality determinations. Final Rule at 39-40.
[4] Final Rule at 29; SEC Form 8-K Item 1.05(a). Note that The SEC will require companies to tag disclosures in Inline XBRL, “including by block text tagging narrative disclosures and detail tagging quantitative amounts.” Final Rule at 88-89.

Contacts

David Aaron
Senior Counsel
Washington, D.C.

Related Services

PRACTICES

- Privacy & Security Law
- Ethics & Compliance

Freshfields

April 11, 2024 | 3 minutes read

CISA Releases Proposed Regulations Implementing New Cybersecurity Reporting Requirements


Brock Dahl
Partner


Beth George
Partner


Timothy Howard
Partner

+3 more...

On April 4, 2024, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") proposed regulations that would create reporting requirements for cyber incidents experienced by critical infrastructure entities. The proposal, a requirement of the 2022-enacted Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), would create a scheme whereby covered entities would be subject to the new reporting requirement if they experience a substantial cyber incident or make a ransomware payment as a result of a ransomware attack. Comments on the proposed rule are due by June 3, 2024.

Covered Entities

All entities in the critical infrastructure sectors are included in the covered entity definition unless designated a “small business” by the Small Business Administration. The 16 critical infrastructure sectors, per Presidential Policy Directive (PPD-21), includes financial services, communications, information technology, commercial facilities, critical manufacturing, and transportation services. Small businesses can still be included as covered entities if they meet sector-based criteria laid out in the proposal. The rule proposal carves out a set of Domain Name System entities from inclusion as covered entities.

Substantial Cyber Incident

Impact Threshold

The proposed definition of substantial cyber incident is triggered if either (1) an impact threshold is met or (2) unauthorized access through a specified third-party entity or supply chain compromise occurs.

The impact threshold for substantial cyber incident designation is met when, regardless of cause, a cyber incident leads to:

- A substantial loss of confidentiality, integrity or availability of a covered entity’s information system or network;
- A serious impact on the safety and resiliency of a covered entity’s operational systems and processes; or
- A disruption of a covered entity’s ability to engage in business or industrial operations, or deliver goods or services.

While the discussion section of the rule proposal does provide a list of “Incidents That Likely Would Not Qualify as Substantial Cyber Incidents”, this list is limited to examples where an entity only experiences minor disruptions or where security controls and

remediation protocols promptly neutralize the risks associated with a cyber incident.

Explicitly Included Cyber Incident Causes

The rule proposal expounds that cyber incidents caused by any of the following events do trigger reporting requirements when the impact threshold is met:

- compromise of a cloud service provider;
- compromise of a managed service provider;
- compromise of another third-party data hosting provider;
- a supply chain compromise;
- a denial-of-service attack;
- a ransomware attack; or
- exploitation of a zero-day vulnerability.

Reporting Requirements

In accordance with CIRCIA, the draft language contemplates mandatory reporting requirements: (1) 72 hours after a covered entity "reasonably believes" that a covered cyber incident has occurred; and (2) 24 hours after ransom payment(s) have been made in response to a ransomware attack. A Joint Covered Cyber Incident and Ransom Payment Report will be made if a ransomware payment has been disbursed by the covered entity prior to the 72-hour deadline for the initial reporting of the covered cyber incident.

Reporting Waiver for Covered Entities with Multiple Requirements

The draft proposal creates a mechanism whereby covered entities which are already required to report relevant cyber incident information to a separate regulator may be waived from notifying CISA directly. The proposal would create "CIRCIA Agreements" which

can be entered into by CISA and another Federal agency, at CISA's determination.

Information Requests and Subpoenas

The Director of CISA is granted the ability to issue information requests and subpoenas in the event of an insufficient response to such a request. The information requests are allowed if the Director has reason to believe that a covered entity experienced a covered cyber incident or made a ransom payment but failed to report it.

Other Key Elements

Records Preservation Requirement

Data and records preservation requirements of the proposal would mandate that information relevant to a covered cyber incident be preserved for at least two years from the date that a reporting obligation starts.

Liability Protections

The proposal does create liability protections whereby litigation solely based on the submission of a CIRCIA Report or a response to a request for information must be promptly dismissed by the court.

“Information Systems” Definition

The proposed language expands on prior definitions of “information systems” to explicitly include operational technology systems such as industrial control systems and programmable logic controllers. The term is used in the reporting criteria requirements of the proposal and its implementation may call for additional information gathering for covered entities accustomed to solely reporting on incidents relating to and affecting software.

Implementation Timeline

CISA currently estimates the Final Rule to be published in late 2025 and for implementation of the regulations to begin in 2026.

Active Preparation

Companies in the critical infrastructure sectors can assess the potential impact of these proposed regulations by examining how the “Substantial Cyber Incident” definition and reporting requirements in the proposal would map to their current incident detection and response protocols. Because the proposed reporting requirements are triggered by an impact threshold, companies defined as covered entities should consider the incorporation of the downstream effects of a cyber incident into their risk review and rating processes. Covered entities should apply a proper scope in assessing which impacts may activate the reporting requirements. The proposed language initiates a reporting requirement when a cyber incident *lead(s) to* one of the enumerated impacts. In practice, this creates a lower reporting threshold than requiring a report when an impact is *caused by* a cyber incident.

Freshfields

November 9, 2023 | 4 minutes read

DFS Expands Scope of Cybersecurity Regulations

Timothy Howard
Partner

Brock Dahl
Partner

Beth George
Partner

+2 more...

Last week, amendments to the New York Department of Financial Services ("DFS") cybersecurity regulations took effect. Codified at 23 NYCRR 500 ("Part 500"), these cybersecurity regulations broadly apply to companies that offer financial services or insurance products in New York state. Part 500 is highly prescriptive, and DFS-licensed entities, including banks, should proactively take steps to review and establish compliance with the new requirements, particularly given DFS history of aggressive enforcement of its cybersecurity regulations.

Highlights of the amendments to the Part 500 cybersecurity regulations include the following:

Enhanced Governance Requirements: Consistent with recent efforts by the Securities and Exchange Commission, Part 500 has intensified cyber governance requirements for covered entities. Among other things, Chief Information Security Officers ("CISOs") are now required to report any significant cybersecurity event or change to the cybersecurity program to the board of directors. In addition, boards of covered entities are obligated to have sufficient cybersecurity-related expertise, which may include the use of advisors, and must exercise oversight over the development, implementation and maintenance of the entity's cybersecurity program, including approving all written policies at least annually.

Multi-Factor Authentication (MFA) Requirements: Although Part 500 further tightens prescriptive security requirements in area number of areas, covered entities should pay particular attention to the updated MFA requirements, given DFS' historical focus of extracting multi-million dollar settlements for failure to comply with that requirement. Previously, MFA implementation was only required for remote access to a covered entity's network. Covered entities are now expected to implement MFA to allow any user to access its information systems, with a limited exception for qualifying small companies, which are only required to implement MFA for remote access to the company's systems, third-party applications that contain the company's non-public information, and privileged accounts. Companies can avoid the MFA requirement if the CISO annually certifies the implementation of reasonably equivalent or more secure compensating controls.

Ransomware and Digital Extortion Focus. Seizing on the dramatic increase in ransomware attacks over the past several years and regulatory concern over payments to the criminal ecosystem, Part 500 imposes an array of new requirements regarding ransomware and digital extortion incidents, including:

- **Backup Requirements**: In order to promote resiliency of information systems in the wake of ransomware attacks, covered entities are now obligated to maintain backups of systems

necessary to restore material operations, and are required to conduct annual tests regarding their ability to restore their systems from backups.

- **Ransomware/Cyber Extortion Reporting Requirements**: Part 500 has historically required notification to DFS of data incidents that either (1) have a material impact on the covered entity's operations or (2) in instances in which the covered entity is otherwise required to report the incident to another regulator. The DFS amendments have added a new notification trigger, where a data incident results in the deployment of ransomware within a material part of the covered entity's information systems. Covered entities are further required to inform DFS within 24 hours of making any payment to a threat actor, and must follow up within 30 days with a report detailing the reasons that payment was necessary, a description of the alternatives to payment considered, all diligence performed to find alternatives to payment, and compliance with other regulations, specifically including the Office of Foreign Assets Control (OFAC). While these requirements do not outlaw payments to threat actors, they significantly raise the stakes for a company that seeks to pay a threat actor by requiring the company to engage in robust, well-documented diligence, particularly surrounding sanctions issues. Further, companies that are contemplating threat actor payments should consider whether the report to DFS would imply a violation of the new Part 500 requirements related to creating available, robust backup systems to restore operations.

Tightened Certification Requirements: Part 500 historically required covered entities to certify compliance on an annual basis but did not provide an alternative option for companies that were not in a position to fully certify compliance. The amendments now make clear that all covered entities are required to either certify compliance or, in the alternative, submit a written acknowledgment that the entity was not in material compliance with all requirements. Any such acknowledgement will be required to identify gaps and provides a remediation timeline. In addition, certifications are

required to be signed by both the CISO and the covered entity's highest-ranking executive. Companies need to pay careful attention to auditing compliance with Part 500, as perceived false or misleading statements in these filings can be used by DFS as the basis for an enforcement action. Further, these certifications increase the risks for signing executives as enforcement authorities are increasingly focused on enforcement actions against individuals related to cybersecurity issues, such as the recent SEC action against SolarWinds executives.

Expanded Obligations for New "Class A" Companies: DFS has also created a new class of large covered entities referred to as "Class A" companies, which are defined as companies with: (a) at least $20 million in gross annual revenue in each of the past two fiscal years in New York State; and (b) either more than 2,000 employees or $1 billion in gross annual revenue for the entity and its affiliates anywhere in the world. Qualifying companies are required to design and conduct independent audits of their cybersecurity program, implement privileged access management solutions, an automated method for blocking commonly used passwords for all accounts, endpoint detection and response solutions to monitor anomalous activity, and centralize logging and security event alerting.

Conclusion. The expanded Part 500 requirements signals an intent by DFS to continue its history of aggressive enforcement of cybersecurity requirements across the wide range of companies that it supervises. Covered entities should pay close attention to the new governance and technical control requirements, and take significant care with compliance certifications in order to minimize the risk of liability to both the covered entities and their certifying officers.

Please note this is not an official version of the Second Amendment to Part 500. There may be formatting and other changes not reflected here. This document is intended to make it easier for regulated persons to identify textual changes made as part of the adoption of the Second Amendment to Part 500.

NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
SECOND AMENDMENT TO 23 NYCRR 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Adrienne A. Harris, Superintendent of Financial Services, pursuant to the authority granted by Sections 102, 201, 202, 301, 302, and 408 of the Financial Services Law, Sections 10, 14, 37(3), 37(4), and 44 of the Banking Law, and Sections 109, 301, 308, 309, 316, 1109, 1119, 1503(b), 1717(b), 2110, and 2127 and Articles 21, 47, and 79 of the Insurance Law, do hereby promulgate the Second Amendment to Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect upon publication of the Notice of Adoption in the State Register, to read as follows:

500.0 Introduction.

The New York State Department of Financial Services (DFS) has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and

estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

500.1 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any person that controls, is controlled by or is under common control with another person. For purposes of this subdivision, *control* means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of stock of such person or otherwise.

(b) *Authorized user* means any employee, contractor, agent or other person that participates in the business operations of a covered entity and is authorized to access and use any information systems and data of the covered entity.

(c) *Chief Information Security Officer* or *CISO* means a qualified individual responsible for overseeing and implementing a covered entity's cybersecurity program and enforcing its cybersecurity policy.

(d) *Class A company* means a covered entity with at least $20,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and the business operations in this State of the covered entity's affiliates and:

> (1) over 2,000 employees averaged over the last two fiscal years, including employees of both the covered entity and all of its affiliates no matter where located; or
>
> (2) over $1,000,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all of its affiliates no matter where located.

For purposes of this subdivision, when calculating the number of employees and gross annual revenue, affiliates shall include only those that share information systems, cybersecurity resources or all or any part of a cybersecurity program with the covered entity.

(e) *Covered entity* means any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies.

(f) *Cybersecurity event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.

(g) *Cybersecurity incident* means a cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that:

(1) impacts the covered entity and requires the covered entity to notify any government body, self-regulatory agency or any other supervisory body;

(2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or

(3) results in the deployment of ransomware within a material part of the covered entity's information systems.

(h) *Independent audit* means an audit conducted by internal or external auditors free to make decisions not influenced by the covered entity being audited or by its owners, managers or employees.

(i) *Information system* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(j) *Multi-factor authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) knowledge factors, such as a password;

(2) possession factors, such as a token; or

(3) inherence factors, such as a biometric characteristic.

(k) *Nonpublic information* means all electronic information that is not publicly available information and is:

(1) business related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity;

(2) any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements:

(i) social security number;

(ii) drivers' license number or non-driver identification card number;

(iii) account number, credit or debit card number;

(iv) any security code, access code or password that would permit access to an individual's financial account; or

(v) biometric records;

(3) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to:

(i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family;

(ii) the provision of health care to any individual; or

(iii) payment for the provision of health care to any individual.

(l) *Penetration testing* means testing the security of information systems by attempting to circumvent or defeat the security features of an information system by authorizing attempted penetration of databases or controls from outside or inside the covered entity's information systems.

(m) *Person* means any individual or entity, including but not limited to any partnership, corporation, branch, agency or association.

(n) *Privileged account* means any authorized user account or service account that can be used to perform security-relevant functions that ordinary users are not authorized to perform, including but not limited to the ability to add, change or remove other accounts, or make configuration changes to information systems.

(o) *Publicly available information* means any information that a covered entity has a reasonable basis to believe is lawfully made available to the general public from: Federal, State or local government records; widely distributed media; or disclosures to the general public that are required to be made by Federal, State or local law. A covered entity has a reasonable basis to believe that information is lawfully made available to the general public if the covered entity has taken steps to determine:

(1) that the information is of the type that is available to the general public; and

(2) whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(p) *Risk assessment* means the process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, customers, consumers, other organizations and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place.

(q) *Senior governing body* means the board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer or officers of a covered

entity responsible for the covered entity's cybersecurity program. For any cybersecurity program or part of a cybersecurity program adopted from an affiliate under section 500.2(d) of this Part, the senior governing body may be that of the affiliate.

(r) *Senior officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a covered entity, including a branch or agency of a foreign banking organization subject to this Part.

(s) *Third-party service provider(s)* means a person that:

(1) is not an affiliate of the covered entity;

(2) is not a governmental entity;

(3) provides services to the covered entity; and

(4) maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity.

500.2 Cybersecurity program.

(a) Each covered entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems and nonpublic information stored on those information systems.

(b) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;

(3) detect cybersecurity events;

(4) respond to identified or detected cybersecurity events to mitigate any negative effects;

(5) recover from cybersecurity events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) Each class A company shall design and conduct independent audits of its cybersecurity program based on its risk assessment.

(d) A covered entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the covered entity.

(e) All documentation and information relevant to the covered entity's cybersecurity program, including the relevant and applicable provisions of a cybersecurity program maintained by an affiliate and adopted by the covered entity, shall be made available to the superintendent upon request.

500.3 Cybersecurity policy.

Each covered entity shall implement and maintain a written policy or policies, approved at least annually by a senior officer or the covered entity's senior governing body for the protection of its information systems and nonpublic information stored on those information systems. Procedures shall be developed, documented and implemented in accordance with the written policy or policies. The cybersecurity policy or policies and procedures shall be based on the covered entity's risk assessment and address, at a minimum, the following areas to the extent applicable to the covered entity's operations:

(a) information security;

(b) data governance, classification and retention;

(c) asset inventory, device management and end of life management;

(d) access controls, including remote access and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security and monitoring;

(h) security awareness and training;

(i) systems and application security and development and quality assurance;

(j) physical security and environmental controls;

(k) customer data privacy;

(l) vendor and third-party service provider management;

(m) risk assessment;

(n) incident response and notification; and

(o) vulnerability management.

500.4 Cybersecurity governance.

(a) Chief information security officer. Each covered entity shall designate a CISO. The CISO may be employed by the covered entity, one of its affiliates or a third-party service provider. If the CISO is employed by a third-party service provider or an affiliate, the covered entity shall:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the covered entity's personnel responsible for direction and oversight of the third-party service provider; and

(3) require the third-party service provider or affiliate to maintain a cybersecurity program that protects the covered entity in accordance with the requirements of this Part.

(b) Report. The CISO of each covered entity shall report in writing at least annually to the senior governing body on the covered entity's cybersecurity program, including to the extent applicable:

(1) the confidentiality of nonpublic information and the integrity and security of the covered entity's information systems;

(2) the covered entity's cybersecurity policies and procedures;

(3) material cybersecurity risks to the covered entity;

(4) overall effectiveness of the covered entity's cybersecurity program;

(5) material cybersecurity events involving the covered entity during the time period addressed by the report; and

(6) plans for remediating material inadequacies.

(c) The CISO shall timely report to the senior governing body or senior officer(s) on material cybersecurity issues, such as significant cybersecurity events and significant changes to the covered entity's cybersecurity program.

(d) The senior governing body of the covered entity shall exercise oversight of the covered entity's cybersecurity risk management, including by:

(1) having sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors;

(2) requiring the covered entity's executive management or its designees to develop, implement and maintain the covered entity's cybersecurity program;

(3) regularly receiving and reviewing management reports about cybersecurity matters; and

(4) confirming that the covered entity's management has allocated sufficient resources to implement and maintain an effective cybersecurity program.

500.5 Vulnerability management.

Each covered entity shall, in accordance with its risk assessment, develop and implement written policies and procedures for vulnerability management that are designed to assess and maintain the effectiveness of its cybersecurity program. These policies and procedures shall be designed to ensure that covered entities:

(a) conduct, at a minimum:

(1) penetration testing of their information systems from both inside and outside the information systems' boundaries by a qualified internal or external party at least annually; and

(2) automated scans of information systems, and a manual review of systems not covered by such scans, for the purpose of discovering, analyzing and reporting vulnerabilities at a frequency determined by the risk assessment, and promptly after any material system changes;

(b) are promptly informed of new security vulnerabilities by having a monitoring process in place; and

(c) timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity.

500.6 Audit trail.

(a) Each covered entity shall securely maintain systems that, to the extent applicable and based on its risk assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the covered entity; and

(2) include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity.

(b) Each covered entity shall maintain records required by paragraph (a)(1) of this section for not fewer than five years and shall maintain records required by paragraph (a)(2) of this section for not fewer than three years.

500.7 Access privileges and management.

(a) As part of its cybersecurity program, based on the covered entity's risk assessment each covered entity shall:

(1) limit user access privileges to information systems that provide access to nonpublic information to only those necessary to perform the user's job;

(2) limit the number of privileged accounts and limit the access functions of privileged accounts to only those necessary to perform the user's job;

(3) limit the use of privileged accounts to only when performing functions requiring the use of such access;

(4) periodically, but at a minimum annually, review all user access privileges and remove or disable accounts and access that are no longer necessary;

(5) disable or securely configure all protocols that permit remote control of devices; and

(6) promptly terminate access following departures.

(b) To the extent passwords are employed as a method of authentication, the covered entity shall implement a written password policy that meets industry standards.

(c) Each class A company shall monitor privileged access activity and shall implement:

(1) a privileged access management solution; and

(2) an automated method of blocking commonly used passwords for all accounts on information systems owned or controlled by the class A company and wherever feasible for all other accounts. To the extent the class A company determines that blocking commonly used passwords is infeasible, the covered entity's CISO may instead approve in writing at least annually the infeasibility and the use of reasonably equivalent or more secure compensating controls.

500.8 Application security.

(a) Each covered entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the covered entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the covered entity within the context of the covered entity's technology environment.

(b) All such procedures, guidelines and standards shall be reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the covered entity at least annually.

500.9 Risk assessment.

(a) Each covered entity shall conduct a periodic risk assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program as required by this Part. Such risk assessment shall be reviewed and updated as reasonably necessary, but at a minimum annually, and whenever a change in the business or technology causes a material change to the covered entity's cyber risk. The covered entity's risk assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems.

(b) The risk assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the covered entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the covered entity's information systems and nonpublic information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

500.10 Cybersecurity personnel and intelligence.

(a) In addition to the requirements set forth in section 500.4(a) of this Part, each covered entity shall:

(1) utilize qualified cybersecurity personnel of the covered entity, an affiliate or a third-party service provider sufficient to manage the covered entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.2(b)(1)–(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A covered entity may choose to utilize an affiliate or qualified third-party service provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in sections 500.4 and 500.11 of this Part.

500.11 Third-party service provider security policy.

(a) Each covered entity shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers. Such policies and procedures shall be based on the risk assessment of the covered entity and shall address to the extent applicable:

(1) the identification and risk assessment of third-party service providers;

(2) minimum cybersecurity practices required to be met by such third-party service providers in order for them to do business with the covered entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third-party service providers; and

(4) periodic assessment of such third-party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to third-party service providers including to the extent applicable guidelines addressing:

(1) the third-party service provider's policies and procedures for access controls, including its use of multi-factor authentication as required by section 500.12 of this Part, to limit access to relevant information systems and nonpublic information;

(2) the third-party service provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect nonpublic information in transit and at rest;

(3) notice to be provided to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or the covered entity's nonpublic information being held by the third-party service provider; and

(4) representations and warranties addressing the third-party service provider's cybersecurity policies and procedures that relate to the security of the covered entity's information systems or nonpublic information.

500.12 Multi-factor authentication.

(a) Multi-factor authentication shall be utilized for any individual accessing any information systems of a covered entity, unless the covered entity qualifies for a limited exemption pursuant to section 500.19(a) of this Part in which case multi-factor authentication shall be utilized for:

(1) remote access to the covered entity's information systems;

(2) remote access to third-party applications, including but not limited to those that are cloud based, from which nonpublic information is accessible; and

(3) all privileged accounts other than service accounts that prohibit interactive login.

(b) If the covered entity has a CISO, the CISO may approve in writing the use of reasonably equivalent or more secure compensating controls. Such controls shall be reviewed periodically, but at a minimum annually.

500.13 Asset management and data retention requirements.

(a) As part of its cybersecurity program, each covered entity shall implement written policies and procedures designed to produce and maintain a complete, accurate and documented asset inventory of the covered entity's information systems. The asset inventory shall be maintained in accordance with written policies and procedures. At a minimum, such policies and procedures shall include:

(1) a method to track key information for each asset, including, as applicable, the following:

(i) owner;

(ii) location;

(iii) classification or sensitivity;

(iv) support expiration date; and

(v) recovery time objectives; and

(2) the frequency required to update and validate the covered entity's asset inventory.

(b) As part of its cybersecurity program, each covered entity shall include policies and procedures for the secure disposal on a periodic basis of any nonpublic information identified in section 500.1(k)(2)–(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the covered entity, except where such information is

otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

500.14 Monitoring and training.

(a) As part of its cybersecurity program, each covered entity shall:

(1) implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, nonpublic information by such authorized users;

(2) implement risk-based controls designed to protect against malicious code, including those that monitor and filter web traffic and electronic mail to block malicious content; and

(3) provide periodic, but at a minimum annual, cybersecurity awareness training that includes social engineering for all personnel that is updated to reflect risks identified by the covered entity in its risk assessment.

(b) Each class A company shall implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls:

(1) an endpoint detection and response solution to monitor anomalous activity, including but not limited to lateral movement; and

(2) a solution that centralizes logging and security event alerting.

500.15 Encryption of nonpublic information.

(a) As part of its cybersecurity program, each covered entity shall implement a written policy requiring encryption that meets industry standards, to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest.

(b) To the extent a covered entity determines that encryption of nonpublic information at rest is infeasible, the covered entity may instead secure such nonpublic information using effective alternative compensating controls that have been reviewed and approved by the covered entity's CISO in writing. The feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

500.16 Incident response and business continuity management.

(a) As part of its cybersecurity program, each covered entity shall establish written plans that contain proactive measures to investigate and mitigate cybersecurity events and to ensure

operational resilience, including but not limited to incident response, business continuity and disaster recovery plans.

(1) Incident response plan. Incident response plans shall be reasonably designed to enable prompt response to, and recovery from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the covered entity's business or operations. Such plans shall address the following areas with respect to different types of cybersecurity events, including disruptive events such as ransomware incidents:

(i) the goals of the incident response plan;

(ii) the internal processes for responding to a cybersecurity event;

(iii) the definition of clear roles, responsibilities and levels of decision-making authority;

(iv) external and internal communications and information sharing;

(v) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(vi) documentation and reporting regarding cybersecurity events and related incident response activities;

(vii) recovery from backups;

(viii) preparation of root cause analysis that describes how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence; and

(ix) updating of incident response plans as necessary.

(2) Business continuity and disaster recovery (BCDR) plan. BCDR plans shall be reasonably designed to ensure the availability and functionality of the covered entity's information systems and material services and protect the covered entity's personnel, assets and nonpublic information in the event of a cybersecurity-related disruption to its normal business activities. Such plans shall, at minimum:

(i) identify documents, data, facilities, infrastructure, services, personnel and competencies essential to the continued operations of the covered entity's business;

(ii) identify the supervisory personnel responsible for implementing each aspect of the BCDR plan;

(iii) include a plan to communicate with essential persons in the event of a cybersecurity-related disruption to the operations of the covered entity, including

employees, counterparties, regulatory authorities, third-party service providers, disaster recovery specialists, the senior governing body and any other persons essential to the recovery of documentation and data and the resumption of operations;

(iv) include procedures for the timely recovery of critical data and information systems and to resume operations as soon as reasonably possible following a cybersecurity-related disruption to normal business activities;

(v) include procedures for backing up or copying, with sufficient frequency, information essential to the operations of the covered entity and storing such information offsite; and

(vi) identify third parties that are necessary to the continued operations of the covered entity's information systems.

(b) Each covered entity shall ensure that current copies of the plans or relevant portions therein are distributed or are otherwise accessible, including during a cybersecurity event, to all employees necessary to implement such plans.

(c) Each covered entity shall provide relevant training to all employees responsible for implementing the plans regarding their roles and responsibilities.

(d) Each covered entity shall periodically, but at a minimum annually, test its:

(1) incident response and BCDR plans with all staff and management critical to the response, and shall revise the plan as necessary; and

(2) ability to restore its critical data and information systems from backups.

(e) Each covered entity shall maintain backups necessary to restore material operations. The backups shall be adequately protected from unauthorized alterations or destruction.

500.17 Notices to superintendent.

(a) Notice of cybersecurity incident.

(1) Each covered entity shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours after determining that a cybersecurity incident has occurred at the covered entity, its affiliates, or a third-party service provider.

(2) Each covered entity shall promptly provide to the superintendent any information requested regarding such incident. Covered entities shall have a continuing obligation to update the superintendent with material changes or new information previously unavailable.

(b) Notice of compliance.

(1) Annually each covered entity shall submit to the superintendent electronically by April 15 either:

(i) a written certification that:

(a) certifies that the covered entity materially complied with the requirements set forth in this Part during the prior calendar year; and

(b) shall be based upon data and documentation sufficient to accurately determine and demonstrate such material compliance, including, to the extent necessary, documentation of officers, employees, representatives, outside vendors and other individuals or entities, as well as other documentation, whether in the form of reports, certifications, schedules or otherwise; or

(ii) a written acknowledgment that:

(a) acknowledges that, for the prior calendar year, the covered entity did not materially comply with all the requirements of this Part;

(b) identifies all sections of this Part that the entity has not materially complied with and describes the nature and extent of such noncompliance; and

(c) provides a remediation timeline or confirmation that remediation has been completed.

(2) Such certification or acknowledgment shall be submitted electronically in the form set forth on the department's website and shall be signed by the covered entity's highest-ranking executive and its CISO. If the covered entity does not have a CISO, the certification or acknowledgment shall be signed by the highest-ranking executive and by the senior officer responsible for the cybersecurity program of the covered entity.

(3) Each covered entity shall maintain for examination and inspection by the department upon request all records, schedules and other documentation and data supporting the certification or acknowledgment for a period of five years, including the identification of all areas, systems and processes that require or required material improvement, updating or redesign, all remedial efforts undertaken to address such areas, systems and processes, and remediation plans and timelines for their implementation.

(c) Notice and explanation of extortion payment. Each covered entity, in the event of an extortion payment made in connection with a cybersecurity event involving the covered entity, shall provide the superintendent electronically, in the form set forth on the department's website, with the following:

(1) within 24 hours of the extortion payment, notice of the payment; and

(2) within 30 days of the extortion payment, a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment and all diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control.

500.18 Confidentiality.

Information provided by a covered entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable State or Federal law.

500.19 Exemptions.

(a) Limited exemption. Each covered entity with:

(1) fewer than 20 employees and independent contractors of the covered entity and its affiliates;

(2) less than $7,500,000 in gross annual revenue in each of the last three fiscal years from all business operations of the covered entity and the business operations in this State of the covered entity's affiliates; or

(3) less than $15,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates,

shall be exempt from the requirements of sections 500.4, 500.5, 500.6, 500.8, 500.10, 500.14(a)(1), (a)(2), and (b), 500.15 and 500.16 of this Part.

(b) An employee, agent, wholly owned subsidiary, representative or designee of a covered entity, who is itself a covered entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, wholly owned subsidiary, representative or designee is covered by the cybersecurity program of the covered entity.

(c) A covered entity that does not directly or indirectly operate, maintain, utilize or control any information systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess nonpublic information shall be exempt from the requirements of sections 500.2, 500.3, 500.4, 500.5, 500.6, 500.7, 500.8, 500.10, 500.12, 500.14, 500.15 and 500.16 of this Part.

(d) A covered entity under article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess nonpublic information other than information relating to its corporate parent company (or affiliates) shall be exempt

from the requirements of sections 500.2, 500.3, 500.4, 500.5, 500.6, 500.7, 500.8, 500.10, 500.12, 500.14, 500.15 and 500.16 of this Part.

(e) An individual insurance broker subject to Insurance Law section 2104 who qualifies for the exemption pursuant to subdivision 500.19(c) of this Part and has not, for any compensation, commission or other thing of value, acted or aided in any manner in soliciting, negotiating or selling any policy or contract or in placing risks or taking out insurance on behalf of another person for at least one year shall be exempt from the requirements of this Part, provided such individuals do not otherwise qualify as a covered entity for purposes of this Part.

(f) A covered entity that qualifies for any of the above exemptions pursuant to this section shall file electronically a Notice of Exemption in the form set forth on the department's website within 30 days of the determination that the covered entity is exempt.

(g) The following persons are exempt from the requirements of this Part, provided such persons do not otherwise qualify as a covered entity for purposes of this Part: persons subject to Insurance Law section 1110; persons subject to Insurance Law section 5904; any accredited reinsurer, certified reinsurer or reciprocal jurisdiction reinsurer that has been so recognized pursuant to 11 NYCRR Part 125; individual insurance agents who are placed in inactive status under Insurance Law section 2103; and individual licensees placed in inactive status under Banking Law section 599-i.

(h) In the event that a covered entity ceases to qualify for an exemption, such covered entity shall have 180 days from the date that it ceases to so qualify to comply with all applicable requirements of this Part.

500.20 Enforcement.

(a) This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

(b) The commission of a single act prohibited by this Part or the failure to act to satisfy an obligation required by this Part shall constitute a violation hereof. Such acts or failures include, without limitation:

> (1) the failure to secure or prevent unauthorized access to an individual's or an entity's nonpublic information due to noncompliance with any section of this Part; or
>
> (2) the material failure to comply for any 24-hour period with any section of this Part.

(c) In assessing any penalty for a violation of this Part pursuant to the Banking Law, Insurance Law or Financial Services Law, the superintendent shall take into account, without limitation, factors including:

> (1) the extent to which the covered entity has cooperated with the superintendent in the investigation of such acts;

(2) the good faith of the entity;

(3) whether the violations resulted from conduct that was unintentional or inadvertent, reckless or intentional and deliberate;

(4) whether the violation was a result of failure to remedy previous examination matters requiring attention, or failing to adhere to any disciplinary letter, letter of instructions or similar;

(5) any history of prior violations;

(6) whether the violation involved an isolated incident, repeat violations, systemic violations or a pattern of violations;

(7) whether the covered entity provided false or misleading information;

(8) the extent of harm to consumers;

(9) whether required, accurate and timely disclosures were made to affected consumers;

(10) the gravity of the violations;

(11) the number of violations and the length of time over which they occurred;

(12) the extent, if any, to which the senior governing body participated therein;

(13) any penalty or sanction imposed by any other regulatory agency;

(14) the financial resources, net worth and annual business volume of the covered entity and its affiliates;

(15) the extent to which the relevant policies and procedures of the company are consistent with nationally recognized cybersecurity frameworks, such as NIST; and

(16) such other matters as justice and the public interest require.

500.21 Effective date.

(a) This Part will be effective March 1, 2017. Covered entities will be required to annually prepare and submit to the superintendent a certification of compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

(b) The second amendment to this Part shall become effective November 1, 2023.

500.22 Transitional periods.

(a) Transitional period.

Covered entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered entities shall have:

(1) one year from the effective date of this Part to comply with the requirements of sections 500.4(b), 500.5, 500.9, 500.12 and 500.14(b) of this Part;

(2) eighteen months from the effective date of this Part to comply with the requirements of sections 500.6, 500.8, 500.13, 500.14(a) and 500.15 of this Part;

(3) two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

(c) Covered entities shall have 180 days from the effective date of the second amendment to this Part to comply with the new requirements set forth in the second amendment to this Part, except as otherwise specified in subdivisions (d) and (e) below.

(d) The following provisions shall include different transitional periods. Covered entities shall have:

(1) 30 days from the effective date of the second amendment to this Part to comply with the new requirements specified in section 500.17 of this Part;

(2) one year from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.4, 500.15, 500.16 and 500.19(a) of this Part;

(3) 18 months from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.5(a)(2), 500.7, 500.14(a)(2) and 500.14(b) of this Part; and

(4) two years from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.12 and 500.13(a) of this Part.

(e) The new requirements specified in sections 500.19(e)-(h), 500.20, 500.21, 500.22 and 500.24 of this Part shall become effective November 1, 2023.

500.23 Severability.

If any provision of this Part or the application thereof to any person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other persons or circumstances.

500.24 Exemptions from electronic filing and submission requirements.

(a) A filer required to make an electronic filing or a submission pursuant to this Part may apply to the superintendent for an exemption from the requirement that the filing or submission be electronic by submitting a written request to the superintendent for approval at least 30 days before the filer shall submit to the superintendent the particular filing or submission that is the subject of the request.

(b) The request for an exemption shall:

(1) set forth the filer's DFS license number, NAIC number, Nationwide Multistate Licensing System number or institution number;

(2) identify the specific filing or submission for which the filer is applying for the exemption;

(3) specify whether the filer is making the request for an exemption based upon undue hardship, impracticability or good cause, and set forth a detailed explanation as to the reason that the superintendent should approve the request; and

(4) specify whether the request for an exemption extends to future filings or submissions, in addition to the specific filing or submission identified in paragraph (2) of this subdivision.

(c) The filer requesting an exemption shall submit, upon the superintendent's request, any additional information necessary for the superintendent to evaluate the filer's request for an exemption.

(d) The filer shall be exempt from the electronic filing or submission requirement upon the superintendent's written determination so exempting the filer, where the determination specifies the basis upon which the superintendent is granting the request and to which filings or submissions the exemption applies.

(e) If the superintendent approves a filer's request for an exemption from the electronic filing or submission requirement, then the filer shall make a filing or submission in a form and manner acceptable to the superintendent.

Appendices A and B to 23 NYCRR 500 are hereby repealed.

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. AND TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 23-cv-9518 Hon. Paul A. Engelmayer

[PROPOSED] BRIEF OF CHIEF INFORMATION SECURITY OFFICERS AND CYBERSECURITY ORGANIZATIONS AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE COMPLAINT

TABLE OF CONTENTS

Page

IDENTITY AND INTERESTS OF *AMICI CURIAE* 1
SUMMARY OF ARGUMENT 1
BACKGROUND 3
ARGUMENT 3
I. CISOs Play an Indispensable Role in Cyber- and National Security 3
A. CISOs Face an Increasingly Challenging Threat Environment 3
B. Flexible Regulatory Frameworks Enable Tailored Cybersecurity Practices 6
C. Cybersecurity Demands Robust Private-Public Collaboration 9
II. The SEC's Claims Are Counterproductive 11
A. The SEC's Claims Could Benefit Threat Actors 11
B. The SEC's Claims Could Exacerbate the Damage Caused by Cyberattacks 12
C. The SEC's Claims Could Chill Internal Discussions and Self-Assessments 15
D. The SEC's Claims Are Likely to Worsen the Critical Shortage of Cybersecurity Professionals 16
E. The SEC's Claims Could Chill Private-Public Cooperation 20
CONCLUSION 22
APPENDIX – LIST OF AMICI CURIAE 22

TABLE OF AUTHORITIES

Cases

Curling v. Raffensperger,
2023 U.S. Dist. LEXIS 202368 (N.D. Ga. Nov. 10, 2023) 6

Statutes

15 U.S.C. 8

18 U.S.C. 8

Cyber Incident Reporting for Critical Infrastructure Act of 2022, 6 U.S.C.
§ 681e(a)(2)(A) 14, 20

Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1505 20

Federal Information Security Management Act, 44 U.S.C. § 3541, et seq. 7

Internet of Things Cybersecurity Act of 2020, 15 U.S.C. § 278g-3c(b) 7

Md. Code Ann., Com. Law § 14-3503(a) (West 2022) 7

N.Y. Comp. Codes R. & Regs. tit. 23, § 500.12(b) 7

Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745 8

Other Authorities

16 C.F.R. § 314.4(c)(5) 7

45 C.F.R. § 164.306(b)(2) 7

The 2023 Fortune 500 CISOs Analysis, FORTIFY EXPERTS (2023),
https://bit.ly/48NQI1f 19

45% of Companies Do Not Employ a CISO, SECURITY MAGAZINE (Nov. 24,
2021) https://bit.ly/3HRQUkt 19

Alicia Hope, *Hackers Compromised Two Large Data Centers in Asia and Leaked Major Tech Giants' Login Credentials*, CPO MAGAZINE (Mar. 8, 2023),
https://bit.ly/48NetGT 4

Alicia Hope, *Healthcare Tech Firm HealthEC Data Breach Impacted Nearly 4.5 Million Patients*, CPO MAGAZINE (Jan. 11, 2024), https://bit.ly/497TKx7 4

Allen D. Householder et al., *The CERT Guide to Coordinated Vulnerability Disclosure*, CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE xi (Aug. 2017), https://bit.ly/3ua2OCT 10, 12

Andi Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter*, Lawfare (Jan. 13, 2021), https://bit.ly/48L7vSN 11

Arnold Lucas Commandeur, *Understanding legacy information systems and abandonment decision making: Towards methodological support* (Mar. 2019) (Ph.D. thesis, University of Groningen, SOM Research School), https://bit.ly/3HI4R4j. 4

Cambrie Eckert, *Just In: U.S. Desperately Needs Cyber Talent, Congress Says*, NATIONAL DEFENSE MAGAZINE 50 (June 26, 2023), https://bit.ly/3vWnKxw 18

Charlie Osborne, *CISO Workforce and Headcount 2023 Report*, CYBERSECURITY VENTURES 8 (2023), https://bit.ly/3HyFjGx 4

Charlotte A. Tschider, Locking Down "Reasonable" 6

Chris Butler, *Lessons from 100+ Ransomware Recoveries*, CPO MAGAZINE (Nov. 6, 2023), https://bit.ly/42jFJdG. 5

CISA, *Coordinated Vulnerability Disclosure Process*, https://bit.ly/42e108v 10, 12

CVE, https://bit.ly/42sl8ne (last visited Feb. 2, 2024) 11

Cyber Incidents: How Best to Work with Law Enforcement, CYBER SECURITY: A PEER-REVIEWED JOURNAL 103 (May 22, 2017), https://bit.ly/3OjzOiR 21

CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T HOMELAND SEC., BINDING OPERATIONAL DIRECTIVE 20-01 (2020), https://bit.ly/42l4c23 7

Cybersecurity & Infrastructure Security Agency ("CISA"), *Defining Insider Threats*, https://bit.ly/4blSjNE (last visited Jan. 18, 2024) 4

Cybersecurity Duty, 41 Yale L. & Pol'y Rev. 75, 80 (2023) 6

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F.R. pts. 22, 232, 240 & 249, Exchange Act Release Nos. 33-11216, 34-97989, SEC Final Rule 65-66 (Sept. 5, 2023), https://bit.ly/42fIBZ6 8

David Yaffe-Bellany, *A Hack of the SEC's Social Media Account Caused a Bitcoin Frenzy, Briefly*, NEW YORK TIMES (Jan. 9, 2024) 6

Deepti Gopal et al., *Predicts 2023: Cybersecurity Industry Focuses on the Human Deal*, GARTNER 61 (Jan. 25, 2023), https://www.bitsight.com/thank-you/gartner-predicts-2023 20

Erastus Karanja & Mark A. Rosso, *The Chief Information Security Officer: An Exploratory Study*, J. of Int'l Tech. & Info. Mgmt.: Vol. 26: Iss. 2, Article 2, SCHOLARWORKS 39 (June 1, 2017), https://bit.ly/3tVLcL2 8

Evolution of the Chief Information Security Officer, THE INSTITUTE OF WORLD POLITICS, https://bit.ly/3S8YE6h (last visited Jan. 17, 2024) 4

Federal Government Cybersecurity Incident & Vulnerability Response Playbooks, CISA (Nov. 2021) https://bit.ly/3SAp8PC 15

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NAT'L INST. OF STANDARDS & TECH. ("NIST") 2 (Apr. 16, 2018), https://bit.ly/3vQqXPr 7, 9

Fredrik Björck et al., *Cyber Resilience - Fundamentals for a Definition*, in 1 NEW CONTRIBUTIONS IN INFORMATION. SYSTEMS & TECHNOLOGIES 311-12 6

Global Cybersecurity Outlook 2023: Insight Report, WORLD ECONOMIC FORUM 12 (Jan. 2023), https://bit.ly/3u8C1a2 2

Growing the National Cybersecurity Talent Pipeline: Hearing Before the Subcomm. on Cybersecurity & Infrastructure Prot. of the H. Comm. on Homeland Sec., 118th Cong. 118-19, 15 .....18, 19

Gurbir S. Grewal, *Remarks at New York City Bar Association Compliance Institute*, SEC (Oct. 24, 2023), https://bit.ly/484SdqV 17

Heidrick & Struggles, 2022 Global Chief Information Security Officer (CISO) Survey 5, https://bit.ly/3SboRRE 19

Henrik Nilsson, *Federal Watchdog Faults Most Agencies' Cybersecurity* (Jan. 9, 2024, 10:08PM), https://bit.ly/3SA9NP2 6

HSDF, *Fireside Chat with CISA Director Jen Easterly and Former Rep. Jim Langevin*, YOUTUBE, at 3:25-4:00 (June 21, 2023), https://bit.ly/48PANzI 10

INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, ISO/IEC 30111 (2019), https://bit.ly/3UimTS5 .....10, 12

INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, ISO/IEC 29147 (2018), https://bit.ly/47VL6ka 10

ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce (2023), https://bit.ly/3Hy9PAl 18

Jon Boyens et al., Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations at 17 (May 2022), U.S. Department of Commerce, Natl. Inst. of Standards & Tech., https://bit.ly/484o7Uh 4

The Journey in Data: HackerOne Hits 100 Million Dollars in Bounties, ETHICAL HACKER (May 28, 2020), https://bit.ly/3UoPV2o 11

Justin Rende, *Attracting and Retaining Top Cybersecurity Talent Amid Worker Burnout and Shortages*, FORBES (Dec. 30, 2022, 6:30 AM), https://bit.ly/48M5TYV 19

Karen Scarfone et al, *Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology* (Sept. 2008) 4

Kevin Townsend, *CISO Conversations: Steve Katz, the World's First CISO*, SECURITYWEEK (Dec. 1, 2021), https://bit.ly/496AzDR 3

Kim Schaffer et al., *Recommendations for Federal Vulnerability Disclosure Guidelines*, NIST SP 800-216, NAT'L INST. STANDARDS & TECH., U.S. DEP'T COM. (May 2023), https://bit.ly/49ddFe0 7

National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Homeland Sec. & Governmental Affs. Comm., Testimony 2 (Sept. 23, 2021) (statement of Jen Easterly, Dir. of CISA), https://bit.ly/3Sv4T5K. 2, 10

National Initiative for Cybersecurity Education, Implementation Plan 9 (2021), https://bit.ly/3HADTeR 18

Neta Oren, *Looking Back at Our Bug Bounty Program in 2022*, META (Dec. 15, 2022), https://bit.ly/3w8otfa 11

Nonprofit Service Provider Blackbaud Settles Data Breach Case for $49.5M with States, ASSOCIATED PRESS (Oct. 5, 2023), https://bit.ly/3Sfj2CA 10

Office of Intelligence & Analysis, *Homeland Threat Assessment*, DHS 18 (2024), https://bit.ly/48MkMue 5

PBSNewsHour, *WATCH: House Hearing on "Worldwide Threats to the Homeland with DHS Secretary Mayorkas*, YouTube, at 2:38:40-2:38:50 (Nov. 15, 2023), https://bit.ly/3vOTaGh 13

Press Release, Gartner, Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025 (Feb. 22, 2023), https://bit.ly/48N3ddp 19

Press Release, National Institute of Standards and Technology, NIST Updates Cybersecurity Guidance for Supply Chain Risk Management (May 5, 2022), https://bit.ly/3Suol2y 4

Press Release, U.S. Att'ys Off., Cent. Dist. of Cal., North Korean Regime-Backed Programmer Charged in Conspiracy to Conduct Multiple Cyberattacks and Intrusions (Sept. 6, 2018), https://bit.ly/3Uwinjd 5

Press Release, U.S. Att'ys Off., S. Dist. of N.Y., Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities (Mar. 24, 2016), https://bit.ly/3OiTl30 5

Press Release, U.S. Att'ys Off., W. Dist. of Penn., U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://bit.ly/3vVzHUc 5

Press Release, U.S. Dep't of Just., Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information (Dec. 20, 2018), https://bit.ly/3OiTbbU 5

Press Release, U.S. Dep't of Just., U.S. Charges Russian FSB Officers and Their Criminal Conspirations for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017), https://bit.ly/42bh3ns 5

Report to the CISA Director: Corporate Cyber Responsibility, CISA Cybersecurity Advisory Committee (Sept. 13, 2023), https://bit.ly/494Yt2H 8

Robert Kemp & Richard Smith, *Security and Safety Incidents and Standards*, CYBER SECURITY: A PEER-REVIEWED JOURNAL (vol. 5, no. 2) 164 (Feb. 2, 2021) 5

Robert S. Mueller, III, U.S. Dep't of Justice, Report on the Investigation into Russian Interference in the 2016 Presidential Election (vol. 1) 50-51 (Mar. 2019), https://bit.ly/42epm23 6

Scott Neuman, *The U.S. Has Formally Accused China of a Massive Cyberattack on Microsoft*, NPR (Jul. 19, 2021), https://bit.ly/48K33Dz 4

Scott Shane et al, *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, NEW YORK TIMES (Nov. 12, 2017) 6

SEC's X Account Hacked, Causing Frenzy Over Bitcoin ETF - The New York Times, SECURITIES DOCKET (Jan. 10, 2024 8:45AM), https://bit.ly/42gXk5N 6

See Secure by Design, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software, CISA 8 (Oct. 2023), https://bit.ly/498bTLq 2

Shaun Bertrand, *SEC SolarWinds Filing: Forecasting the Fallout for CISOs*, CONVERGE TECHNOLOGY SOLUTIONS (Dec. 14, 2023), https://bit.ly/47U5ulQ.....19

Testimony of Christopher A. Wray, Dir., Fed. Bureau Investigations, Worldwide Threats to the Homeland Before the Comm. on Homeland Sec., 118th Cong., at 5 (Nov. 15, 2023), https://bit.ly/42a4mtd.....5, 14, 20

U.S. Cybersecurity Group, *The Evolving Role of the CISO: More Than Just Security*, ASPEN INSTITUTE 2 (Oct. 2023), https://bit.ly/48NF8mH 4

U.S. Dep't of Defense, Directive No. 8000.01, Management of the Dep't of Defense Information Enterprise 3 (July 27, 2017), https://bit.ly/3Ui3Lnd.....18

U.S. Dep't of Justice, Cybersecurity Unit, Criminal Division, Best Practices for Victim Response and Reporting of Cyber Incidents 1, https://bit.ly/3HvXzQP ..... *passim*

U.S. Department of Commerce, Natl. Inst. of Standards & Tech., https://bit.ly/3Ov2o0G 4

U.S. SEC. & EXCH. COMM'N, *Cybersecurity Risk Management, Strategy, Governance, and Incident*, https://bit.ly/48PAxRg (last visited Jan. 25, 2024) 8

White Paper – CISO's Guide to Sensitive Data Protection: An Application Security Viewpoint, SYNOPSYS 3-4 (Mar. 2021), https://bit.ly/3HGn81U.....4

IDENTITY AND INTERESTS OF *AMICI CURIAE*

Amici are thirty professionals and entities with vast experience in cybersecurity.[2] Individual amici include current and former Chief Information Security Officers ("CISOs") and other senior cybersecurity professionals employed by public and private organizations across the United States, all of whom are signing the Brief in their individual capacities. Organizational amici represent or advise organizations, CISOs, and other cybersecurity professionals on cybersecurity governance, risk, and mitigation, and collectively represent the interests of hundreds of CISOs and the broader cybersecurity community. Given their firsthand day-to-day experience with novel cybersecurity risks, vulnerabilities, threats, and cyberattacks, amici have great concerns that, based on the alleged facts in the Complaint, the SEC's unprecedented theories of liability against SolarWinds Corporation ("SolarWinds") and its CISO may culminate in harmful consequences for cybersecurity and U.S. national security.

SUMMARY OF ARGUMENT

An organization's information security team, led by its CISO, stands on the front lines against cyberattacks from criminal enterprises, insider threats, "hackers," non-state actors, and hostile foreign governments seeking to steal personal data or intellectual property, hold organizations hostage, compromise critical infrastructure, and undermine U.S. national security. Defending against these threats, CISOs and their teams serve as engineers safeguarding IT infrastructure; intelligence officers identifying and mitigating new vulnerabilities; compliance experts navigating regulations; advisors educating organizational leadership; and—when a cyber incident occurs—emergency responders assessing and containing the damage, protecting

[2] The identities, titles, and affiliations of amici are provided in the Appendix. Amici affirm that no counsel for a party authored this Brief in whole or in part and that no person other than amici, their members, or their counsel made a monetary contribution intended to fund the Brief's preparation or submission.

organizational and third-party assets, patching software, and engaging with victims, other organizations, and the Government in defense of cyber- and national security.

The private sector operates the "vast majority" of IT systems in the United States and the risk of cyberattacks continues to grow.[3] In the war between cyber-attackers and defenders, "attackers have a structural advantage: they need to find only one exploitable weakness" using a limitless array of strategies and tools, whereas organizations must defend against evolving threats on multiple fronts.[4] As the Cybersecurity and Infrastructure Security Agency ("CISA") recognizes, not even the best-resourced CISO can guarantee success against 100% of sophisticated attacks.[5]

Amici, who represent entities and individuals with vast experience on the front lines of this global battlefield, submit this Brief based on their deep concern about the negative impact of the SEC's claims. The SEC's theories propose to sanction SolarWinds and Timothy G. Brown based on internal communications aimed at improving cybersecurity, as well as alleged inadequacies in public filings, which CISOs are not typically responsible for drafting or approving. Liability under these theories empowers threat actors, chills internal communications about cyber-threats, exacerbates the already severe shortage of cybersecurity professionals, and deters collaboration between the private sector and the Government. Amici respectfully submit that the SEC's claims, if allowed to proceed, could significantly harm U.S. cyber- and national defense.

---

[3] *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Homeland Sec. & Governmental Affs. Comm.*, Testimony 2 (Sept. 23, 2021) (statement of Jen Easterly, Dir. of CISA), https://bit.ly/3Sv4T5K.

[4] *Global Cybersecurity Outlook 2023: Insight Report*, WORLD ECONOMIC FORUM 12 (Jan. 2023), https://bit.ly/3u8C1a2.

[5] *See Secure by Design, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*, CISA 8 (Oct. 2023), https://bit.ly/498bTLq.

BACKGROUND

Between 2019 and 2020, the Russian government and its affiliates engaged in cyberattacks against SolarWinds. On December 14, 2020, shortly after learning that it had fallen victim to such an attack—one of the most sophisticated in history—SolarWinds disclosed this news in a Form 8-K. In January 2021, Mr. Brown—who previously served as SolarWinds' Vice President of Security Architecture—became SolarWinds' CISO.

On October 30, 2023, the SEC filed a Complaint alleging that Mr. Brown and SolarWinds made materially misleading statements or omissions about cybersecurity risks and vulnerabilities in: (i) a "Security Statement" posted to the company's website before Mr. Brown and SolarWinds knew of the cyberattack; (ii) Form S-1 and S-8 Registration Statements filed with the SEC before they knew the cyberattack; and (iii) the Form 8-K disclosing the attack. In its allegations, the SEC contrasts the company's public statements with Mr. Brown's internal discussions, in which he sought to keep SolarWinds executives informed about risks and progress on security initiatives.

ARGUMENT

I. CISOs Play an Indispensable Role in Cyber- and National Security

A. CISOs Face an Increasingly Challenging Threat Environment

The CISO position emerged in 1995 when Citibank, reeling from a cyberattack, hired its first specialized cybersecurity executive.[6] Companies had historically delegated IT-related responsibilities to their Chief Information Officer ("CIO"). Yet CIOs mainly focused on IT infrastructure and not the unique challenges of cybersecurity.[7] As companies responded to "the

[6] Kevin Townsend, *CISO Conversations: Steve Katz, the World's First CISO*, SECURITYWEEK (Dec. 1, 2021), https://bit.ly/496AzDR.

[7] *Id.*

ever-increasing need to maintain the security of information and operations,"[8] the CISO role grew more common. Today, over 7,500 CISOs are employed in the United States,[9] although, as noted below, many positions are unfilled due to a shortage of qualified cybersecurity professionals.

Although each CISO role is different based on their organization's unique needs, all CISOs manage evolving cybersecurity risks against necessary tradeoffs.[10] For example, CISOs commonly manage risks associated with modifying or replacing a legacy information system, when doing so may disrupt operations and divert resources;[11] protecting customer and user privacy;[12] conducting penetration testing that may identify new risks but divert engineers from other pressing security priorities;[13] and deciding how to engage with third-party systems that may create risks for the organization's own systems.[14] In addition to these day-to-day risks, CISOs also face actual or attempted security breaches, including insider abuses and external cyberattacks.[15]

---

[8] *Evolution of the Chief Information Security Officer*, THE INSTITUTE OF WORLD POLITICS, https://bit.ly/3S8YE6h (last visited Jan. 17, 2024).

[9] Charlie Osborne, *CISO Workforce and Headcount 2023 Report*, CYBERSECURITY VENTURES 8 (2023), https://bit.ly/3HyFjGx.

[10] *See* U.S. Cybersecurity Group, *The Evolving Role of the CISO: More Than Just Security*, ASPEN INSTITUTE 2 (Oct. 2023), https://bit.ly/48NF8mH.

[11] *See generally* Arnold Lucas Commandeur, *Understanding legacy information systems and abandonment decision making: Towards methodological support* (Mar. 2019) (Ph.D. thesis, University of Groningen, SOM Research School), https://bit.ly/3HI4R4j.

[12] *White Paper – CISO's Guide to Sensitive Data Protection: An Application Security Viewpoint*, SYNOPSYS 3-4 (Mar. 2021), https://bit.ly/3HGn81U.

[13] *See* Karen Scarfone et al, *Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology*, NATL. INST. OF STANDARDS & TECH. 2-1 (Sept. 2008), https://bit.ly/3Ov2o0G ("[T]ime, staff, hardware, and software, resource availability [are] often a limiting factor in . . . security assessments.").

[14] *See generally* Jon Boyens et al., *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NATL. INST. OF STANDARDS & TECH. 17 (May 2022), https://bit.ly/484o7Uh.

[15] *See, e.g.*, Press Release, National Institute of Standards and Technology, NIST Updates Cybersecurity Guidance for Supply Chain Risk Management (May 5, 2022), https://bit.ly/3Suol2y; Cybersecurity & Infrastructure Security Agency ("CISA"), *Defining Insider Threats*, https://bit.ly/4blSjNE (last visited Jan. 18, 2024); Alicia Hope, *Hackers Compromised Two Large Data Centers in Asia and Leaked Major Tech Giants' Login Credentials*, CPO MAGAZINE (Mar. 8, 2023), https://bit.ly/48NetGT; Scott Neuman, *The U.S. Has Formally Accused China of a Massive Cyberattack on Microsoft*, NPR (Jul. 19, 2021), https://bit.ly/48K33Dz; Alicia Hope, *Healthcare Tech Firm HealthEC Data Breach Impacted Nearly 4.5 Million Patients*, CPO MAGAZINE (Jan. 11, 2024), https://bit.ly/497TKx7; Chris Butler, *Lessons from 100+ Ransomware Recoveries*, CPO MAGAZINE (Nov. 6, 2023), https://bit.ly/42jFJdG.

In managing risks, CISOs must deal with the threat of hostile foreign governments sponsoring cyberattacks against U.S. organizations. FBI Director Christopher Wray recently testified: "[W]e have seen the People's Republic of China ("PRC"), the Democratic People's Republic of Korea ("DPRK"), and Russia use cyber operations to target U.S. research."[16] In turn, the U.S. Department of Justice ("DOJ") has indicted individuals for cyberattacks associated with hostile powers like China,[17] Russia,[18] Iran,[19] and North Korea.[20] Defending against such sophisticated foreign-sponsored attacks requires a constant arms race between CISOs and persistent, well-funded adversaries.[21] As on any other battlefield, decisions are made in dynamic situations with incomplete information and no guarantee of perfect security.[22] Under these fog-of-war conditions, CISOs and their teams must triage a steady stream of potential threats while recognizing that ultimately, "[a]ny Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack."[23]

---

[16] Testimony of Christopher A. Wray, Dir., Fed. Bureau Investigations, Worldwide Threats to the Homeland Before the Comm. on Homeland Sec., 118th Cong., at 5 (Nov. 15, 2023), https://bit.ly/42a4mtd.

[17] *See* Press Release, U.S. Dep't of Just., Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information (Dec. 20, 2018), https://bit.ly/3OiTbbU; Press Release, U.S. Att'ys Off., W. Dist. of Penn., U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://bit.ly/3vVzHUc.

[18] *See* Press Release, U.S. Dep't of Just., U.S. Charges Russian FSB Officers and Their Criminal Conspirations for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017), https://bit.ly/42bh3ns.

[19] *See* Press Release, U.S. Att'ys Off., S. Dist. of N.Y., Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities (Mar. 24, 2016), https://bit.ly/3OiTl30.

[20] *See* Press Release, U.S. Att'ys Off., Cent. Dist. of Cal., North Korean Regime-Backed Programmer Charged in Conspiracy to Conduct Multiple Cyberattacks and Intrusions (Sept. 6, 2018), https://bit.ly/3Uwinjd.

[21] Novel technologies, including artificial intelligence, are already being weaponized by threat actors against U.S. companies and the Government. *See* Office of Intelligence & Analysis, *Homeland Threat Assessment*, DHS 18 (2024), https://bit.ly/48MkMue.

[22] Robert Kemp & Richard Smith, *Security and Safety Incidents and Standards*, CYBER SECURITY: A PEER-REVIEWED JOURNAL (vol. 5, no. 2) 164 (Feb. 2, 2021) ("Often the victims of these attacks turn out to be compliant with a number of security standards.").

[23] U.S. Dep't of Justice, Cybersecurity Unit, Criminal Division, Best Practices for Victim Response and Reporting of Cyber Incidents 1, https://bit.ly/3HvXzQP.

The Government is no exception. Even the SEC and the nation's most sophisticated intelligence agencies such as the National Security Agency, have fallen prey to cyberattacks.[24] During the 2016 election cycle, for example, "18 states were the subject of cyberattacks" by foreign adversaries and other threat actors.[25] Many federal agencies have "mostly ineffective" cyber defenses, according to a January 2024 report by the U.S. Government Accountability Office.[26] Given this reality, "the cybersecurity world has shifted to . . . 'cyber resilience'"—accepting "that cyberattacks will continue and cannot be fully avoided."[27]

B. Flexible Regulatory Frameworks Enable Tailored Cybersecurity Practices

To date, most regulatory regimes have wisely avoided prescriptive "one-size-fits-all" approaches to cybersecurity governance. Instead, they have offered CISOs frameworks to triage risks. Amici know from their own experiences that a flexible approach is required to distinguish between acceptable and unacceptable cybersecurity risks in light of competing tradeoffs and resource constraints. The SEC's action against Mr. Brown threatens to undermine this flexibility, which regulators—including the SEC itself—have recognized as essential.

For example, the federal National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF") is a leading guide, followed voluntarily by many public and

---

[24] *See, e.g.*, Scott Shane et al, *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, NEW YORK TIMES (Nov. 12, 2017); *SEC's X Account Hacked, Causing Frenzy Over Bitcoin ETF – The New York Times*, SECURITIES DOCKET (Jan. 10, 2024 8:45AM), https://bit.ly/42gXk5N (citing David Yaffe-Bellany, *A Hack of the SEC's Social Media Account Caused a Bitcoin Frenzy, Briefly*, NEW YORK TIMES (Jan. 9, 2024)).

[25] *Curling v. Raffensperger*, 2023 U.S. Dist. LEXIS 202368, at *119–21 (N.D. Ga. Nov. 10, 2023); *see* Robert S. Mueller, III, U.S. Dep't of Justice, Report on the Investigation into Russian Interference in the 2016 Presidential Election (vol. 1) 50–51 (Mar. 2019), https://bit.ly/42epm23 (detailing Russian cyberattacks against state- and county-level election administration).

[26] Henrik Nilsson, *Federal Watchdog Faults Most Agencies' Cybersecurity*, Law360 (Jan. 9, 2024, 10:08PM), https://bit.ly/3SA9NP2.

[27] Charlotte A. Tschider, Locking Down "Reasonable" Cybersecurity Duty, 41 Yale L. & Pol'y Rev. 75, 80 (2023) (citing Fredrik Björck et al., *Cyber Resilience - Fundamentals for a Definition*, in 1 NEW CONTRIBUTIONS IN INFORMATION SYSTEMS & TECHNOLOGIES 311-12).

private organizations.[28] The CSF recognizes that each organization has "different threats . . . vulnerabilities, [and] . . . risk tolerances," and that there is no "one-size-fits-all approach to managing cybersecurity risk for critical infrastructure."[29] The CSF gives utmost flexibility to CISOs based on their distinct organizational needs and constraints.

Federal and state regulations also seek to maximize flexibility in organizations' approaches to cybersecurity.[30] Even prescriptive rules in these regulatory schemes afford significant discretion, such as exempting organizations from multi-factor authentication protocols if the CISO "approve[d] in writing the use of reasonably equivalent or more secure compensating controls."[31]

The CISO role is evolving. One study noted that "[t]here is a lack of consensus regarding the scope of the [CISO] position, the duties, and its place in the organizational hierarchy."[32] CISOs appear to occupy senior positions, but their role is distinct in compensation, authority, and reporting lines from core C-suite executives. CISOs' authority and communication lines within a

[28] *See* Federal Information Security Management Act, 44 U.S.C. § 3541, et seq.

[29] *See Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NAT'L INST. OF STANDARDS & TECH. ("NIST") 2 (Apr. 16, 2018), https://bit.ly/3vQqXPr.

[30] *See, e.g.*, Internet of Things Cybersecurity Act of 2020, 15 U.S.C. § 278g-3c(b) (establishing federal guidelines "to be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization or any other appropriate, relevant, and widely-used standard"); CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T HOMELAND SEC., BINDING OPERATIONAL DIRECTIVE 20-01, at 3–7 (2020), https://bit.ly/42l4c23; Kim Schaffer et al., *Recommendations for Federal Vulnerability Disclosure Guidelines*, NIST SP 800-216, NAT'L INST. STANDARDS & TECH., U.S. DEP'T COM. (May 2023), https://bit.ly/49ddFe0.

[31] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.12(b); *cf.* 16 C.F.R. § 314.4(c)(5). Similarly, federal health regulations provide a non-exhaustive list of factors that covered entities must consider for data security, without specifying any particular measure they must adopt. *See* 45 C.F.R. § 164.306(b)(2) (factors include "[t]he size, complexity, and capabilities of the covered entity or business associate," "[t]he covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities," "[t]he costs of security measures," and "[t]he probability and criticality of potential risks to electronic protected health information"). And many state-level regulations frame cybersecurity in terms of reasonableness, without defining or enumerating which security measures would qualify as reasonable. *See, e.g.*, Md. Code Ann., Com. Law § 14-3503(a) (West 2022) (requiring businesses to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned, maintained, or licensed and the nature and size of the business and its operations").

[32] Erastus Karanja & Mark A. Rosso, *The Chief Information Security Officer: An Exploratory Study*, J. of Int'l Tech. & Info. Mgmt.: Vol. 26: Iss. 2, Article 2, SCHOLARWORKS 39 (June 1, 2017), https://bit.ly/3tVLcL2.

company are often not commensurate with the responsibilities they are expected to fulfill.[33] And though senior management benefits from regulations and guidance promulgated under the Sarbanes-Oxley Act for a company's financial operations, Congress has never adopted a comparable law governing CISOs and cybersecurity.[34]

Even the SEC has struggled to articulate the expected duties of CISOs under its current statutory authority, as shown by proposed amendments to its final rule on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."[35] After the notice-and-comment process, the SEC backtracked on its proposed rule that companies disclose "whether and how the board integrates cybersecurity into its business strategy, risk management, and financial oversight," as well as "whether the company has a [CISO] or someone in a comparable position, and if so, to whom the individual reports within the registrant's organizational chart."[36] Instead, the final rule now avoids "inadvertently pressur[ing] registrants to adopt specific or inflexible cybersecurity-risk governance practices or organizational structures."[37] These changes underscore that regulators, including the SEC, have deliberately abstained from establishing a prescriptive set of rules for cybersecurity governance.

In light of the flexibility built into federal and state authorities, the SEC's stance here—that an organization and its CISO commit securities fraud for claiming to "follow" the NIST CSF

[33] *See* Report to the CISA Director: Corporate Cyber Responsibility, CISA Cybersecurity Advisory Committee (Sept. 13, 2023), https://bit.ly/494Yt2H ("Cyberattacks and their impact could be better mitigated or even prevented if corporate boards of directors were more educated and engaged on matters relating to cybersecurity, placed a higher priority on cyber resilience, and exercised stronger oversight over the development and execution of their companies' cybersecurity strategies.").

[34] *See* Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745 (codified in scattered sections of 15 and 18 U.S.C.).

[35] U.S. SEC. & EXCH. COMM'N, *Cybersecurity Risk Management, Strategy, Governance, and Incident*, https://bit.ly/48PAxRg (last visited Jan. 25, 2024).

[36] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F.R. pts. 22, 232, 240 & 249, Exchange Act Release Nos. 33-11216, 34-97989, SEC Final Rule 65-66 (Sept. 5, 2023), https://bit.ly/42fIBZ6.

[37] *See id.* at 70-71.

if they identify vulnerabilities through self-assessments under "the NIST Framework"[38]—makes no sense.[39] Indeed, the SEC's attempt to effectively penalize an organization and its CISO for supposedly negative findings in NIST self-assessments undermines the key objective of the CSF to "support self-assessment of investment effectiveness and cybersecurity activities."[40] The CSF expressly recognizes that risk management is inherently iterative, and that measuring "an organization's cybersecurity state and trends *over time* can enable that organization to understand and convey meaningful risk information to dependents, suppliers, buyers, and other parties."[41] In other words, routine self-monitoring confirms a company's good-faith attempt to implement the Framework and iteratively build cyber resilience. The SEC wrongly seeks to punish Mr. Brown for industry-standard practice for CISOs: identifying risks through self-assessments and using those results to bolster cybersecurity.

C. Cybersecurity Demands Robust Private-Public Collaboration

CISOs operate within a "cybersecurity ecosystem" that relies on increasing information-sharing among and between organizations and the Government to guard against novel threats. Information infrastructures are increasingly interconnected (for example, through cloud service providers or other data management contractors) such that a security breach in any one organization's systems can affect the data of thousands of others.[42] As a result, on top of their internal duties, CISOs must engage with the broader cybersecurity ecosystem in which their organizations are enmeshed. And because the private sector operates the "vast majority" of IT

[38] Complaint ¶ 45.

[39] *See* ECF No. 46 at 22-24.

[40] NIST CSF, § 4.0.

[41] *Framework for Improving Critical Infrastructure Cybersecurity*, *supra* note 29 at 20.

[42] *See, e.g.*, *Nonprofit Service Provider Blackbaud Settles Data Breach Case for $49.5M with States*, ASSOCIATED PRESS (Oct. 5, 2023), https://bit.ly/3Sfj2CA (sensitive information, including health information and social security numbers of over 13,000 nonprofits exposed in 2020 breach of software provider).

systems in the United States, CISA recognizes that it must work with the private sector to "create trusted valued partnerships through transparency [and] responsiveness" that encourage no-blame information sharing regarding cyber risks and attacks.[43] As CISA director Jen Easterly put it, "cyber[security] is a team sport."[44]

Questions about how to share or publicize information about a particular vulnerability are highly sensitive and require team-wide consideration of tradeoffs and follow-on effects, because, among other things, "[n]otifying the public that a problem exists without offering a specific course of action to remediate it can result in giving an adversary the advantage while the remediation gap persists."[45] Thus, programs like CISA's coordinated vulnerability disclosure process permit private companies to report vulnerabilities in software products to the agency in confidence, which then coordinates disclosure while considering the potential effects of the vulnerability on critical infrastructure and "availability of effective mitigations."[46] As detailed below, *see* Section II.C *infra*, the SEC's claims could chill this critical cooperation, as CISOs would need to weigh whether disclosing a vulnerability or breach to Government partners could increase their risk of personal liability, adding new layers of risk to an already difficult business decision.

---

[43] HSDF, *Fireside Chat with CISA Director Jen Easterly and Former Rep. Jim Langevin*, YOUTUBE, at 3:25–4:00 (June 21, 2023), https://bit.ly/48PANzI.

[44] *National Cybersecurity Strategy*, statement by Jen Easterly, *supra* note 3 at 2.

[45] Allen D. Householder et al., *The CERT Guide to Coordinated Vulnerability Disclosure*, CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE xi (Aug. 2017), https://bit.ly/3ua2OCT; *accord* INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, ISO/IEC 30111 (2019) https://bit.ly/3UimTS5; INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, ISO/IEC 29147 (2018), https://bit.ly/47VL6ka.

[46] *See* CISA, *Coordinated Vulnerability Disclosure Process*, https://bit.ly/42e108v (last visited Jan. 17, 2024). Likewise, the Vulnerability Equities Process, first developed by the White House in 2017, "outlines the procedure through which the government weighs various considerations in determining when to disclose software vulnerabilities and when to exploit them for law enforcement or foreign intelligence purposes" in consultation with multiple government stakeholders. Andi Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter*, Lawfare (Jan. 13, 2021), https://bit.ly/48L7vSN.

II. The SEC's Claims Are Counterproductive

A. The SEC's Claims Could Benefit Threat Actors

The SEC seeks to hold Mr. Brown personally liable for allegedly insufficient detail about vulnerabilities in SolarWinds's information system in SEC filings. *See* Compl. (ECF No. 1) ¶¶ 175–77 (implying that, to avoid liability, SolarWinds should have "disclose[d] the numerous risks, vulnerabilities, and incidents affecting its products in its SEC filings"). But, by virtue of their responsibilities, CISOs engage with countless, novel "risks" and "vulnerabilities" daily. For example, organizations commonly conduct "penetration testing" to probe their systems for weaknesses, which virtually always result in some findings of risks and vulnerabilities. These findings take time to fix due to technical complexity and resource constraints, and remain open issues in the meantime. As another example, many organizations operate bug bounty programs, which incentivize "white hat" security researchers to find vulnerabilities in their software products, resulting in dozens, hundreds, or even thousands of vulnerability reports through these channels.[47] As yet another, organizations often use third-party software, in which its manufacturers discover risks and offer patches, which take time to implement across organizations.[48]

These are only several examples of the many types of risks that CISOs must manage daily. It is plainly impracticable and, amici submit, impossible to expect a CISO or company to detail all major risks and vulnerabilities in public SEC filings. No organization's cybersecurity is perfect. At any given moment, organizations identify new cybersecurity risks and have hundreds, if not

[47] *See, e.g.*, Neta Oren, *Looking Back at Our Bug Bounty Program in 2022*, META (Dec. 15, 2022), https://bit.ly/3w8otfa (explaining that Facebook has received "more than 170,000 reports" through its bug bounty program since 2011); *The Journey in Data: HackerOne Hits 100 Million Dollars in Bounties*, ETHICAL HACKER (May 28, 2020) https://bit.ly/42sl8ne (reporting that the HackerOne service that many companies use to receive bug bounty reports receives 40 vulnerability reports every 100 minutes).

[48] For example, in 2023 alone, over 28,000 such vulnerabilities were publicly reported by software companies through the what is known as the CVE Program. *See* CVE, https://bit.ly/42sl8ne (last visited Feb. 2, 2024).

thousands, of ongoing vulnerabilities that they are working to mitigate in real-time. And as soon as one set of critical risks is resolved, others are virtually certain to arise because the vulnerability landscape is continuously changing and requires constant internal reassessment and scaffolding of risks, based on tradeoffs, priorities, and other constraints.

Requiring organizations to provide detailed public disclosures of vulnerabilities would also result in harmful impact across the cybersecurity ecosystem. Consider a cloud company hosting sensitive data from thousands of persons, organizations, and Government agencies. Disclosures revealing the company's vulnerabilities would provide a trove of useful intelligence to threat actors interested in exploiting those vulnerabilities. That risk in turn could potentially harm the cloud company and all others whose data the company hosts. Publicizing such information near to real-time would be impractical, dangerous, and a radical departure from best practice.

For that very reason, CISA's coordinated vulnerability disclosure process for third-party software that may affect other companies calls for "sufficient time for affected users to obtain, test, and apply mitigation strategies prior to public disclosure."[49] Despite this recommendation by the Government's main cybersecurity agency, the SEC's theory of liability here would give CISOs and companies an incentive to make premature and detailed disclosures before mitigation strategies have been carried out—to the benefit of threat actors.

B. The SEC's Claims Could Exacerbate the Damage Caused by Cyberattacks

The SEC's theory of liability concerning public disclosures *during* a cyberattack also runs counter to Government-endorsed best practices. *See* Compl. ¶¶ 182–93 (suggesting that SolarWinds should have publicly disclosed that the ongoing cyberattacks "definitively allowed the attacker to compromise the server on which the Orion products were running" and allowed for

[49] *Coordinated Vulnerability Disclosure Process*, *supra* note 46; *see also* ISO/IEC 30111, *supra* note 48; ISO/IEO 29147, *supra* note 48; Householder, *supra* note 45.

"infiltration of customers' systems"). For example, DOJ's Best Practices for Cyber Victims emphasize that, "[d]uring an intrusion, an organization's management and personnel should be focused on containing the intrusion, mitigating the harm, and collecting and preserving vital information that will help them assess the nature and scope of the damage and the potential source of the threat."[50] The guidance lays out a multi-step process for a cyberattack response: (1) conduct an initial assessment; (2) minimize continuing damage; (3) collect information; and finally (4) notify employees, law enforcement, DHS, regulators, and other victims.[51]

DOJ's Best Practices for Cyber Victims recommends cyberattack victims take steps to "minimize continuing damage."[52] CISOs concerned about potential personal liability during an attack will be distracted from this urgent task. Recognizing this issue, during a recent hearing before the House Committee on Homeland Security, Congresswoman Yvette Clarke admonished the Government for subjecting cyberattack victims to contradictory reporting requirements that "undermine security . . . [due to] a disproportionate focus on compliance with various reporting regulations over security and incident response."[53] The FBI Director echoed those sentiments, testifying that, during "cyber incidents [such as] SolarWinds," the Government should speak with "one voice" and not impose contradictory reporting requirements.[54]

Ignoring these concerns, the SEC faults SolarWinds for simply stating in its initial disclosure that it was "still investigating" an issue, asserting this was "false" given that Mr. Brown already had formed a belief about that issue. *See, e.g.*, Compl. ¶¶ 189–90. The SEC's allegations

[50] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 23 at 2.

[51] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 23 at 14.

[52] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 23 at 7.

[53] PBSNewsHour, *WATCH: House Hearing on "Worldwide Threats to the Homeland with DHS Secretary Mayorkas*, YouTube, at 2:38:40–2:38:50 (Nov. 15, 2023), https://bit.ly/3vOTaGh (statement of Rep. Clarke).

[54] Testimony of Christopher A. Wray, Dir., Fed. Bureau Investigations, *Worldwide Threats to the Homeland Before the Comm. on Homeland Sec.*, 118th Cong., at 7 (Nov. 15, 2023), https://bit.ly/42a4mtd.

fail to appreciate the fast-paced and uncertain nature of breach investigations, and presume that preliminary beliefs of individual incident response team members are established facts to be disclosed immediately, rather than issues that may require further investigation and validation.

Detailed early disclosures during an ongoing attack or its immediate, chaotic aftermath would compromise cybersecurity. CISOs who believe that oversharing information in public disclosures protects them and their organizations against claims of material omissions could have an incentive to disregard DOJ guidance to "not disclose incident-specific information" to any outside party other than the Government and other known victims.[55] This is particularly true while Government investigations into a breach are ongoing. "The FBI and U.S. Secret Service will . . . conduct their investigations with discretion and work with a victim company to ***avoid unwarranted disclosure of information***. . . . Victim companies should likewise consider sharing press releases regarding a cyber incident with investigative agents before issuing them ***to avoid releasing information that might damage the ongoing investigation***."[56]

Discretion is prudent because "[i]t is possible that, despite best efforts, a company that has addressed known security vulnerabilities and taken all reasonable steps to eject an intruder has nevertheless not eliminated all of the means by which the intruder illicitly accessed the network."[57] Under those conditions, disclosing detailed "incident-specific information" in a public filing may provide valuable intelligence to the attacker, showing what the organization knows and does not know about the breach. Such details could also prove useful to other threat actors, who may

[55] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 23 at 12.

[56] *Id.* at 10-11 (emphasis added); see also Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), 6 U.S.C. § 681e(a)(2)(A) (Upon receiving a report regarding "an ongoing cyber threat or security vulnerability," CISA will "identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.").

[57] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 23 at 13.

"actively monitor defensive response measures and shift their methods to evade detection and containment,"[58] and could target the breached organization or test other organizations for similar vulnerabilities. By charging Mr. Brown under the facts alleged here, the SEC neglects to consider the harmful consequences of premature disclosure, putting CISOs in the impossible position of having to weigh future liability against immediate security needs.

C. The SEC's Claims Could Chill Internal Discussions and Self-Assessments

The SEC cites internal communications among Mr. Brown and other employees discussing areas for improvement or noting one-off deviations from SolarWinds' cybersecurity policies. *See* Compl. ¶¶ 77–112, 194–202 (contrasting SolarWinds's policies on access controls, strong passwords, and VPNs, with one-off instances of noncompliance). But this approach fails to recognize candid, real-time communications between a CISO and organizational leadership are essential to developing and maintaining effective cybersecurity. The fact that a CISO, or a member of their team, identifies specific deviations from their company's policies does not indicate that the CISO negligently failed to address compliance, or that the company does not maintain and use those policies. Cybersecurity professionals reading a public disclosure—such as the SolarWinds Security Statement at issue here—would understand that it is not intended to convey any guarantee of perfect security or compliance.

Maintaining any organizational policy involves identifying and rectifying deficiencies, and candid discussions between CISOs, their teams, and organizational leadership are essential for any cybersecurity program seeking to mitigate risk. The SEC's attempt to weaponize Mr. Brown's presentations to higher-ups alerting them to cybersecurity risks cannot be reconciled with its insistence that Mr. Brown "failed to ensure" that "senior executives were sufficiently aware of, or

[58] *Federal Government Cybersecurity Incident & Vulnerability Response Playbooks*, CISA (Nov. 2021) https://bit.ly/3SAp8PC.

understood, the severity of" the risks identified in those briefings. Compl. ¶ 100. And by using such communications as a basis for personal liability for Mr. Brown, the SEC's action could chill (and, in some cases, probably already has chilled) necessary and open discussion about cyberthreats within organizations. Indeed, the SEC's action would give CISOs an incentive to refrain from candid communication for fear that an internal email or presentation intended to improve cybersecurity measures will be taken out of context by the SEC to claim that a CISO deliberately misled investors.

The SEC's action could also discourage CISOs from conducting routine cybersecurity assessments—including those recommended by the NIST Framework—that could alert them to new vulnerabilities, for fear of discovering information that the SEC would say must be disclosed publicly, particularly before remediation can be fully addressed. Compl. ¶¶ 49–53, 65 (citing vulnerabilities identified in voluntary NIST self-assessments as a basis for Mr. Brown's liability). Transparency is especially vital in the "all-hands-on-deck" situation of a breach, and concerns about personal liability will hinder efforts to resolve the crisis.

In short, the SEC's action could incentivize CISOs to avoid discussing and investigating risks internally while also giving an incentive to overstate and overshare potential vulnerabilities in SEC disclosures. This, in turn, would hamstring CISOs in the arms race by undermining the work of detecting and improving vulnerabilities, stifle the flow of important information about cyber risks within an organization, while also tipping off hackers, thereby increasing the likelihood of a successful cyberattack.

D. The SEC's Claims Are Likely to Worsen the Critical Shortage of Cybersecurity Professionals

The SEC's claims against Mr. Brown are the *first time* a cybersecurity professional faces personal liability for alleged public material misrepresentations for, in effect, doing their job.

Under the SEC's theories, a CISO who enforces a company's policies by maintaining open lines of communication with their team about potential compliance gaps allegedly commits fraud by failing to disclose those gaps to the public. Compl. ¶¶ 7–9, 62 (alleging that SolarWinds's public "cybersecurity risk disclosure[s]" were too "generic and hypothetical," unlike internal discussions identifying cybersecurity risks and working to mitigate them). The SEC ultimately premises liability on routine aspects of a CISO's job: trying to defend their organization against threat actors, conducting self-assessments, notifying senior executives about risks, taking proactive steps to resolve such risks, and establishing cybersecurity practices that the organization endeavors to implement.[59] Compl. ¶¶ 7–9, 49–53, 62, 65, 77–112, 182–202. These new theories of liability are likely to cause more CISOs to leave their positions and deter qualified individuals from entering the profession, thereby exacerbating an acute shortage of cybersecurity professionals.

The dearth of cybersecurity professionals is already so severe as to threaten U.S. national security. Indeed, the U.S. Department of Defense has identified the cybersecurity workforce gap"—the difference between the number of cybersecurity personnel organizations require versus the number available for hire—as a critical priority.[60] The International Information System Security Certification Consortium ("ISC2") estimates a gap of 4 million globally and 482,985 in

[59] In other contexts involving compliance professionals, the SEC's practice has been *not* to pursue actions unless the "misconduct [is] unrelated to the compliance function," or where there is a "wholesale failure" to carry out their duties. Gurbir S. Grewal, *Remarks at New York City Bar Association Compliance Institute*, SEC (Oct. 24, 2023), https://bit.ly/484SdqV.

[60] U.S. Dep't of Defense, Directive No. 8000.01, Management of the Dep't of Defense Information Enterprise 3 (July 27, 2017), https://bit.ly/3Ui3Lnd (emphasizing the need to cultivate a "highly qualified and capable cyberspace workforce"). The National Initiative for Cybersecurity Education's 2021–2025 Strategic Plan also calls for private-public collaboration to "recruit, hire, develop, and retain the talent needed to manage cybersecurity-related risks." National Initiative for Cybersecurity Education, Implementation Plan 9 (2021), https://bit.ly/3HADTeR.

the United States.[61] In a recent hearing before the House Homeland Security Committee's Subcommittee on Cybersecurity and Infrastructure Protection, a witness testified about that gap:

> [T]here are over 660,000 cybersecurity job openings in the United States, but we only have 69 skilled cybersecurity workers for every 100 that employers demand[.] . . . [W]e are stepping onto the digital battlefield missing nearly a third of our army, and the consequences of this talent shortage echo across our country.[62]

Mr. Markow added that "annual demand for cybersecurity workers has grown 200 percent in the past 10 years. Such rapid growth is difficult for our education system to catch up with in any field, let alone one as technically demanding and dynamic as cybersecurity."[63] Over 40% of cybersecurity professionals report that their organizations face difficulties in hiring and retaining individuals with the necessary skills.[64] This workforce gap helps explain why most cybersecurity professionals believe their organizations are at "extreme" or "moderate risk" of a cyberattack.[65]

The workforce gap is most acutely manifest in vacant cybersecurity leadership roles. Largely because of the difficulty in finding qualified CISOs, nearly half (45%) of companies surveyed did not employ a CISO,[66] including 19% (94) of Fortune 500 companies.[67] Organizations hiring across all industries face a severe lack of CISO candidates.[68] Without a qualified CISO on staff, organizations face near insurmountable hurdles in managing sophisticated cyberattacks.

---

[61] *See ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce*, ISC2 12 (2023), https://bit.ly/3Hy9PAl.

[62] *See* Cambrie Eckert, *Just In: U.S. Desperately Needs Cyber Talent, Congress Says*, NATIONAL DEFENSE MAGAZINE 50 (June 26, 2023), https://bit.ly/3vWnKxw.

[63] *Growing the National Cybersecurity Talent Pipeline: Hearing Before the Subcomm. on Cybersecurity & Infrastructure Prot. of the H. Comm. on Homeland Sec.*, 118th Cong. 118-19, 15 (statement of Will Markow) (2023).

[64] *See ISC2 Cybersecurity Workforce Study*, *supra* note 61 at 24.

[65] *ISC2 Cybersecurity Workforce Study*, *supra* note 61 at 26.

[66] *45% of Companies Do Not Employ a CISO*, SECURITY MAGAZINE (Nov. 24, 2021) https://bit.ly/3HRQUkt.

[67] *The 2023 Fortune 500 CISOs Analysis*, FORTIFY EXPERTS (2023), https://bit.ly/48NQI1f.

[68] Justin Rende, *Attracting and Retaining Top Cybersecurity Talent Amid Worker Burnout and Shortages*, FORBES (Dec. 30, 2022, 6:30 AM), https://bit.ly/48M5TYV.

Apart from hiring, organizations also struggle to retain their existing CISOs. Surveys show that average CISO tenure is less than five years.[69] The cause for high attrition is apparent:

> Cybersecurity professionals are facing unsustainable levels of stress. . . . CISOs are on the defense, with the only possible outcomes that they don't get hacked or they do. The psychological impact of this directly affects decision quality and the performance of cybersecurity leaders and their teams.[70]

In a 2022 study, over half of CISOs surveyed reported that their current CISO roles saddled them with "significant personal risks," including "stress," "burnout," "personal financial accountability for a breach," and "job loss as a result of a breach."[71] Approximately 25% of CISOs expect to leave the CISO role entirely due to these overlapping "work-related stressors."[72]

One CISO described the ramifications of the SEC case as follows:

> For CISOs already contemplating leaving their role, the SEC's charges will only add fuel to their desire to get out. Others feeling pressure or low support from their board of directors or C-level management will likely strongly consider moving on now. . . . [T]here will be attrition related to the CISO role, either by CISOs already in a similar position as Tim Brown or those who want to be sure not to head there.[73]

More and more CISOs, as well as other cybersecurity leaders, are likely to opt out of a role in which they can be held personally responsible by the SEC based on issues outside of their control and beyond their reasonable ability to defend against in the case of nation-state attackers.[74]

---

[69] Heidrick & Struggles, 2022 Global Chief Information Security Officer (CISO) Survey 5, https://bit.ly/3SboRRE.

[70] Press Release, Gartner, Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025 (Feb. 22, 2023), https://bit.ly/48N3ddp.

[71] Heidrick & Struggles, *supra* note 69 at 12; *Growing the National Cybersecurity Talent Pipeline*, *supra* note 63 at 3 (statement of Rep. Garbarino, Chair, H. Comm. on Homeland Security) ("61 percent of those who are employed [as cybersecurity professionals] say they are burned out after triaging years of major cyber incidents.").

[72] Press Release, Gartner, *supra* note 70.

[73] Shaun Bertrand, *SEC SolarWinds Filing: Forecasting the Fallout for CISOs*, CONVERGE TECHNOLOGY SOLUTIONS (Dec. 14, 2023), https://bit.ly/47U5ulQ.

[74] *Cf.* Deepti Gopal, et al., *Predicts 2023: Cybersecurity Industry Focuses on the Human Deal*, GARTNER 61 (Jan. 25, 2023), https://www.bitsight.com/thank-you/gartner-predicts-2023 (noting that employee "churn will damage the [cybersecurity] mission and cost more").

E. The SEC's Claims Could Chill Private-Public Cooperation

Just as dangerous, the SEC's action could deter cooperation with law enforcement and CISA. Many CISOs proactively, and quietly, cooperate with the Government when they learn about new risks. As FBI Director Wray emphasized:

> [The Government] need[s] the private sector to come forward and warn us and our partners when they see malicious cyber activity. We also need the private sector to work with us when we warn them that they are being targeted. Significant cyber incidents—SolarWinds, Cyclops Blink, the Colonial pipeline incident—only emphasize what we have been saying for a long time: the government cannot protect against cyber threats on its own.[75]

Private-public cooperation on cybersecurity is so essential that Congress expressly prohibits CISA from weaponizing voluntary cyberattack disclosures "to regulate [the disclosing organization], including through an enforcement action."[76]

Along similar lines, DOJ recommends that organizations "establish a relationship with their local federal law enforcement offices long before they suffer a cyber incident" since such a "trusted relationship . . . cultivates bi-directional information sharing that is beneficial both to potential victim organizations and to law enforcement."[77] As DOJ acknowledges, when "deciding whether to notify law enforcement of a cyber incident or whether to cooperate fully in an investigation, organisations [and CISOs] weigh the anticipated benefits of a proactive approach against legal, business, reputational and other practical concerns."[78]

---

[75] Testimony of Christopher A. Wray, Dir., Fed. Bureau Investigations, *Worldwide Threats to the Homeland Before the Comm. on Homeland Sec.*, 118th Cong., at 7 (Nov. 15, 2023), https://bit.ly/42a4mtd.

[76] CIRCIA, 6 U.S.C. § 681e(a)(5)(A); *id.* § 681e(b)–(c) (providing protections for cyberattack reporting); *see* Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1505 (protecting organizations from liability if they follow voluntary cybersecurity monitoring and disclosure practices). The law is replete with examples of the Government's express recognition that risk of personal liability reasonably deters victims from reporting crimes and cooperating with law enforcement (*e.g.*, U Visas for victims of criminal activity, safe haven laws, safe harbor laws).

[77] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 23 at 5.

[78] *Cyber Incidents: How Best to Work with Law Enforcement*, CYBER SECURITY: A PEER-REVIEWED JOURNAL 103 (May 22, 2017), https://bit.ly/3OjzOiR.

Knowing that they may be unfairly and disproportionately exposed to personal liability rather than treated as a victim could deter CISOs from creating a "trusted relationship" with the Government. In deciding whether to disclose to law enforcement (1) known vulnerabilities seeking technical assistance; (2) attempted cyberattacks to share best practices; or (3) successful breaches, to prevent the further compromise of sensitive information and even national security, CISOs must grapple with mounting concerns that they are handing over incomplete evidence that the SEC may later weaponize against them. Even if information is turned over, any delay to assess the risk of individual liability may seriously hinder investigations into the perpetrators.

Faced with potential liability under the SEC's theories here, the CISO of, for example, a chip company whose technology powers millions of computers and phones, would face a dilemma when discovering a new vulnerability. Rather than sharing what they know with the Government, they may seek to minimize potential SEC liability by either (i) choosing not to share any details with law enforcement, for fear of being accused of not simultaneously disclosing complete information to the investing public, or (ii) waiting to share information with law enforcement only when it can also safely be described in contemporaneous public filings, at which point law enforcement would be deprived of the benefit of early threat intelligence. Both choices undermine the cybersecurity ecosystem and tilt the board in favor of persistent threat actors. Accordingly, the SEC's action risks disrupting a robust history of private-public information-sharing and is in stark tension with the collaborative best practices of other federal agencies like CISA, the FBI and DOJ, and with cybersecurity more broadly.

CONCLUSION

For these reasons, the claims against Mr. Brown and SolarWinds should be dismissed.

February 2, 2024

Respectfully submitted,

/s/ Andrew D. Goldstein

Timothy T. Howard (4333233)
Robert Barton (5862545)*
Susannah Benjamin (5924402)*
FRESHFIELDS BRUCKHAUS DERINGER US LLP
601 Lexington Avenue, 31st Floor
New York, NY 10022
Phone: (212) 277-4000
Email: timothy.howard@freshfields.com
robert.barton@freshfields.com
susannah.benjamin@freshfields.com

* Application pending for admission to the U.S. District Court for the Southern District of New York

Andrew D. Goldstein (4585675)
COOLEY LLP
55 Hudson Yards
New York, NY 10001-2157
Phone: (212) 479-6000
Email: agoldstein@cooley.com

Josef T. Ansorge (5353081)
Matt K. Nguyen (admitted *pro hac vice*)
Robert H. Denniston (admitted *pro hac vice*)
COOLEY LLP
1299 Pennsylvania Ave., NW, Suite 700
Washington, DC 20004
Phone: (202) 842-7800
Email: jansorge@cooley.com
mnguyen@cooley.com
rdenniston@cooley.com

Counsel for amici curiae Chief Information Security Officers and Cybersecurity Organizations

APPENDIX — LIST OF AMICI CURIAE

ORGANIZATIONAL AMICI:

The **Cyber Governance Alliance (CGA)** is a coalition of experienced cyber professionals representing stakeholders throughout the critical infrastructure ecosystem and is committed to proactive solutions that protect and empower the cyber community. CGA educates policymakers about the importance of principles-based cyber governance solutions and believes those acting in good faith and in accordance with accepted best practices should be guaranteed liability protections under the law.

The **GlobalCISO Leadership Foundation (GCLF)** is an independent, CISO-led foundation that aims to advance mentor-driven, quality education for cybersecurity professionals.

The **Internet Security Alliance (ISA)** is a cross-sector trade group with membership from virtually every critical industry sector. Its mission is to integrate advanced technology with economics and public policy to create a sustainably secure cyber system. It is a recognized world leader in developing and promoting independently assessed and proven-effective cybersecurity risk management principles, toolkits and best practices.

The Petrie Group provides cybersecurity consulting support to small businesses.

The **Secure Policy Coalition**, owned and operated by Modern Fortis LLC, is a strategic alliance dedicated to the support of CISOs, cyber professionals, corporations, and stakeholders.

The **Security Innovation Network (SINET)** is a trusted and purpose-driven community that accelerates the investments and the advancement of early stage and emerging growth cybersecurity companies into global markets. Its model connects cybersecurity, CISO, risk executives, and professionals from venture capital, investment banking, system integration, policy, legal, academia and science, as well as international government, civilian, military and intelligence agencies.

TAG Infosphere is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to provide on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science.

INDIVIDUAL AMICI[79]:

Chirag Arora, former CISO, Crum & Forster; Chair, GlobalCISO Leadership Foundation Advisory Board

Louis Bobelis, Deputy CISO and Head of Security Operations, AXIS Capital

Amy Bogac, former CISO, The Clorox Company

Sandy Buchanan, Managing Director and former Chief Security Officer, Mirai Security, Inc.

Joanna Burkey, former CISO, HP Inc.; former CISO, Siemens Americas

Emily Elaine Coyle, former Head of U.S. Cybersecurity and Privacy Policy, SAP N.A.; former Co-Leader, Cyber Policy & Consumer Privacy Engagement Programs, Ernst & Young, LLP; President, Cyber Governance Alliance

Amit Elazari, former Head of Cybersecurity Policy, Intel Corp.; CEO and Co-Founder, OpenPolicy

Steven Foley, CISO, Exelon Corp.

Brian Fricke, CISO, City National Bank of Florida; former CISO, City National Bank; former CISO, BBVA USA; former CISO, Bank OZK

Brian Harrell, VP and Chief Security Officer, Avangrid, Inc.; former Assistant Secretary for Infrastructure Protection, U.S. Department of Homeland Security; former Assistant Director for Infrastructure Security, U.S. Cybersecurity & Infrastructure Agency

Jay Leek, former CISO, The Blackstone Group; Managing Partner, SYN Ventures

Izak Mutlu, former CISO, Salesforce, Inc.

Jon Miller, CEO, Halcyon

Aaron Nasi, Senior Director of Cybersecurity, Albertsons Companies

[79] Individual *amici* have signed this Brief in their personal capacities and not on behalf of any affiliated institutions. Titles and institutional affiliations are for identification purposes only.

John Petrie, former CISO, NTT Security Inc.; former CISO, Harland Clarke Holdings Corporation; former CISO, The University of Texas Health Science Center at San Antonio

Michael Rosen, Strategic Advisor, NightDragon

Mike Stango, Executive Director, Security50

Andrew Smeaton, former CISO, DataRobot, Inc.

Seth Spergel, Managing Partner, Merlin Ventures

Brett Wahlin, CISO, Activision Blizzard; former CISO, Amazon Prime Video; former CISO, Staples; former CISO, Hewlett-Packard

Laura Whitt-Winyard, VP of Security, Hummingbird; former CISO, Malwarebytes; former CISO, DLL Group

Steve Williams, Global CISO, NTT DATA, Inc.; former CISO, Advanced Micro Devices, Inc.

Allen Wilson, CISO, Axis Capital

CERTIFICATE OF SERVICE

I hereby certify that on February 2, 2024, I electronically filed this document with the Court via CM/ECF, which will automatically send notice and a copy of same to counsel of record via email.

/s/ *Andrew D. Goldstein*
Andrew D. Goldstein