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. 1:23-cv-9518 Hon. Paul A. Engelmayer

MOTION OF CHIEF INFORMATION SECURITY OFFICERS AND CYBERSECURITY ORGANIZATIONS FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE AMENDED COMPLAINT

Pursuant to the Court's order dated December 27, 2023 (ECF No. 38), Chief Information Security Officers ("CISOs") and Cybersecurity Organizations respectfully request leave of this Court to file the attached Brief as *amicus curiae* in support of Defendants' renewed motion to dismiss the SEC's Amended Complaint. ECF No. 88. The Court previously granted amici's motion for leave to file an earlier brief supporting dismissal of the SEC's original complaint. ECF Nos. 70, 83. The SEC does not oppose the instant motion.

Amici are over fifty individuals and entities with vast experience in cybersecurity.[1] In the proposed Brief, amici seek to aid the Court's consideration of Defendants' renewed motion to dismiss by informing the Court about the potential impact of the SEC's action on cybersecurity professionals, including CISOs, as well as the impact on cybersecurity and national security more broadly. In particular, the Brief explains how the SEC's theories of liability are counterproductive given the real-world demands of cybersecurity, and risk harmful consequences, including elevating the frequency and harm of cyberattacks, impeding internal efforts to bolster cybersecurity, worsening the CISO hiring and retention crisis, and deterring CISOs from cooperating with the Government. Amici submit that the SEC's claims, if permitted to proceed under the facts as alleged in its Amended Complaint, are likely to undermine cybersecurity and national security.

[1] The identities, titles, and affiliations of individual and organizational amici are provided in the Brief Appendix.

For these reasons, amici respectfully request the permission to file the attached Brief.

March 29, 2024

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

Timothy T. Howard (4333233)
Robert Barton (5862545)
Susannah Benjamin (5924402)
FRESHFIELDS BRUCKHAUS DERINGER US LLP
World Trade Center, 175 Greenwich Street
New York, NY 10007
Phone: (212) 277-4000
Email: timothy.howard@freshfields.com
robert.barton@freshfields.com
susannah.benjamin@freshfields.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

CERTIFICATE OF SERVICE

I hereby certify that on March 29, 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

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. 1:23-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 AMENDED COMPLAINT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

TABLE OF AUTHORITIES
continued

Page(s)

TABLE OF AUTHORITIES
continued

Page(s)

TABLE OF AUTHORITIES
continued

Page(s)

TABLE OF AUTHORITIES
continued

Page(s)

TABLE OF AUTHORITIES
continued

Page(s)

IDENTITY AND INTERESTS OF *AMICI CURIAE*

Amici are over fifty professionals and entities with vast experience in cybersecurity.[1] 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 the SEC's unprecedented theories of liability against SolarWinds Corporation ("SolarWinds") and its CISO may have 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

[1] 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.[2] CISOs draw on inherently flexible cybersecurity frameworks to iteratively improve their organizations' practices and mitigate the frequency and severity of cyberattacks. Still, 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, while organizations must defend against evolving threats on multiple fronts.[3] As the Cybersecurity and Infrastructure Security Agency ("CISA") recognizes, not even the best-resourced CISO can prevent 100% of sophisticated attacks.[4]

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. Much like the SEC's original complaint, the Amended Complaint ("AC") disregards "the customs and practices" of the cybersecurity profession and the limitations of the CISO position.[5] It proposes 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. The AC also points to SolarWinds' alleged failure to "follow" the National Institute of Standards and Technology ("NIST") Cybersecurity Framework—even as that framework is inherently flexible and non-

---

[2] *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Homeland Sec. & Governmental Affs. Comm.*, 117th Cong. 2 (2021) (statement of Jen Easterly, Dir., Cybersec. & Infrastructure Sec. Agency), https://bit.ly/3Sv4T5K.

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

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

[5] *In re Philip Morris Int'l Inc. Sec. Litig.*, 2021 WL 4135059, at *11 (S.D.N.Y. Sept. 10, 2021) (citation omitted).

prescriptive. Liability under these theories could empower threat actors, chill internal communications about cyber-threats, exacerbate the already severe shortage of cybersecurity professionals, and deter 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.

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 its original complaint. After Defendants moved to dismiss and several interested parties, including amici, filed briefs supporting dismissal, the SEC filed the AC on February 16, 2024. The AC expands on the SEC's prior allegations 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) SEC Form S-1 and S-8 Registration Statements filed before they knew of the cyberattack; and (iii) SEC Form 8-K Reports disclosing the attack. In its amended allegations, the SEC contrasts the company's public statements with Mr. Brown's internal discussions, in which he sought to enforce SolarWinds' cybersecurity policies and keep 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 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

---

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

[7] *Id.*

[8] *Evolution of the Chief Information Security Officer*, INST. WORLD POL., https://bit.ly/3S8YE6h (last visited Mar. 26, 2024).

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

[10] *See The Evolving Role of the CISO: More Than Just Security*, U.S. CYBERSEC. GROUP, ASPEN INST. 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. dissertation, Univ. of Groningen, SOM Rsch. Sch.), https://bit.ly/3HI4R4j.

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

priorities;[13] and deciding how to engage with third-party systems that may create risks for the organization's own systems.[14] Along with these day-to-day risks, CISOs also face actual or attempted security breaches, including insider abuses and external cyberattacks.[15]

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."[16] 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 company are often not commensurate with the responsibilities they are expected to fulfill.[17] As the National Cyber Director has recognized, CISOs do "not always get to decide what technology and security capabilities they work with"—instead, their job is to mitigate the risk of decisions other executives have already made.[18] CISOs typically play no role in investor relations or a company's SEC filings. And though senior management benefits from regulations and guidance promulgated

---

[13] *See* Karen Scarfone et al., *Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology*, NAT'L INST. OF STANDARDS & TECH. ("NIST") 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*, NIST 17 (May 2022), https://bit.ly/484o7Uh.

[15] *See, e.g.*, Press Release, NIST, NIST Updates Cybersecurity Guidance for Supply Chain Risk Management (May 5, 2022), https://bit.ly/3Suol2y; 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 MAG. (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 MAG. (Jan. 11, 2024), https://bit.ly/497TKx7; Chris Butler, *Lessons from 100+ Ransomware Recoveries*, CPO MAG. (Nov. 6, 2023), https://bit.ly/42jFJdG.

[16] Erastus Karanja & Mark A. Rosso, *The Chief Information Security Officer: An Exploratory Study*, 26 J. INT'L TECH. & INFO. MGMT. 23, 39 (Feb. 1, 2017), https://bit.ly/3tVLcL2.

[17] *See* CISA, Cybersec. Advisory Comm., *Report to the CISA Director: Corporate Cyber Responsibility* (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.").

[18] Off. Nat'l Cyber Director, The White House, *Back to the Building Blocks: A Path Toward Secure and Measurable Software* 14 (Feb. 2024), https://bit.ly/3VfmmAR.

under the Sarbanes-Oxley Act for a company's financial operations, Congress has never adopted a comparable law governing CISOs and cybersecurity.[19]

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 that "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."[20] In turn, the U.S. Department of Justice ("DOJ") has indicted individuals for cyberattacks associated with hostile powers like China,[21] Russia,[22] Iran,[23] and North Korea.[24] Defending against such sophisticated foreign-sponsored attacks requires a constant arms race between CISOs and persistent, well-funded adversaries.[25] As on any other battlefield, decisions are made in dynamic situations with incomplete information and no guarantee of perfect security.[26] Under these fog-of-war conditions, CISOs and their teams must triage a steady stream of potential threats while recognizing that

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

[20] *Worldwide Threats to the Homeland: Hearing Before the H. Comm. on Homeland Sec.*, 118th Cong. 5 (2023) (statement of Christopher A. Wray, Dir., Fed. Bureau Investigations), https://bit.ly/42a4mtd.

[21] *See* Press Release, U.S. Dep't 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. 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.

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

[23] *See* Press Release, U.S. Att'ys Off., S. Dist. 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.

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

[25] Novel technologies, including artificial intelligence, are already being weaponized by threat actors against U.S. companies and the Government. *See* U.S. Dep't Homeland Sec., Off. of Intel. & Analysis, Homeland Threat Assessment, 18 (2024), https://bit.ly/48MkMue.

[26] Robert Kemp & Richard Smith, *Security and Safety Incidents and Standards*, 5 CYBER SEC. 164 (Feb. 2, 2021) ("Often the victims of these attacks turn out to be compliant with a number of security standards.").

ultimately, "[a]ny Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack."[27]

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.[28] During the 2016 election cycle, for example, "18 states were the subject of cyberattacks" by foreign adversaries and other threat actors.[29] Many federal agencies have "mostly ineffective" cyber defenses, according to a January 2024 report by the U.S. Government Accountability Office.[30] Given this reality, "the cybersecurity world has shifted to . . . 'cyber resilience'"—accepting "that cyberattacks will continue and cannot be fully avoided."[31]

B. SUNBURST Was One of the Most Sophisticated Cyberattacks in History

The sophistication of SUNBURST exemplifies the challenges that CISOs and their organizations face in the modern cyberthreat landscape. On February 5, 2021, following an extensive investigation, CISA reported the following findings on SUNBURST. Perpetrated by Russian government-sponsored hackers, SUNBURST was a "trojan horse" attack,[32] where hackers hide malicious code in software that appears to be legitimate. A typical "trojan horse" could be

---

[27] U.S. Dep't Just., Cybersec. Unit, Crim. Div., Best Practices for Victim Response and Reporting of Cyber Incidents (Ver. 1.0) 1 (Apr. 2015), https://bit.ly/3HvXzQP.

[28] *See, e.g.*, Scott Shane et al., *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, N.Y. TIMES (Nov. 12, 2017); David Yaffe-Bellany, *A Hack of the SEC's Social Media Account Caused a Bitcoin Frenzy, Briefly*, N.Y. TIMES (Jan. 9, 2024).

[29] *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 Just., 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).

[30] Henrik Nilsson, *Federal Watchdog Faults Most Agencies' Cybersecurity*, LAW360 (Jan. 9, 2024, 10:08 PM), https://bit.ly/3SA9NP2.

[31] 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).

[32] CISA, *Analysis Report: MAR-10318845-1.v1—SUNBURST* (Apr. 15, 2021), https://bit.ly/3ItP2hS. A Trojan Horse is a type of malware that is disguised as a legitimate program. *Trojan Horse Virus*, FORTINET, https://bit.ly/3T8Awkz (last visited Mar. 8. 2024).

found in a malicious attachment appended to a phishing email. In this case, however, the hackers used a far more novel and sophisticated set of tactics. They inserted malicious code directly into versions of Orion shortly before distribution to customers in a way that avoided systems designed to catch such unintended changes.[33] They were thus able to embed malicious code in updates to SolarWinds' Orion software that customers would download directly from SolarWinds onto their own servers that would run Orion—and to do so in a way that was difficult for either SolarWinds or its customers to detect.

SUNBURST was also designed to be difficult to detect even after download. The perpetrators programmed SUNBURST to lie dormant for up to two weeks on an Orion server after being downloaded.[34] Once activated, SUNBURST performed several checks on the Orion server to determine whether any security tools (*e.g.*, antivirus software) were active.[35] If it detected the presence of any such tools, SUNBURST temporarily shut down to avoid detection and worked to deactivate that tool during the next power cycle.[36]

SUNBURST then connected to and communicated with a "Command and Control" (or "C2") server[37] to alert the Russian hackers that SUNBURST was present on the compromised Orion server. After establishing that connection, the perpetrators could attempt to leverage SUNBURST as a backdoor into the customer's broader network environment. The perpetrators programmed SUNBURST to gather information about the compromised Orion server, which it

---

[33] CrowdStrike Intelligence Team, *SUNSPOT: An Implant in the Build Process*, CROWDSTRIKE (Jan. 11, 2021), https://bit.ly/3vkKqb7.

[34] *Analysis Report: MAR-10318845-1.v1—SUNBURST*, *supra* note 32.

[35] *Id.*

[36] Stephen Eckels et al., *SUNBURST Additional Technical Details*, MANDIANT BLOG (Oct. 28, 2021), https://bit.ly/4a2lPGK.

[37] A "Command and Control" server allows hackers to remotely send commands to and receive data from a server that has been infected by malware. Bart Lenaerts-Bergmans, *What Are Command and Control (C&C) Attacks?*, CROWDSTRIKE (July 20, 2023), https://bit.ly/4a6l7If.

would include as part of the information sent to the C2 server.[38] To avoid arousing suspicion, the perpetrators programmed SUNBURST to disguise its communications with the hackers' C2 Server as if they were communications with SolarWinds' "Orion Improvement Program," or "OIP"—a program SolarWinds ran to gather usage information from customers for product improvement purposes.[39] In short, the SUNBURST attack was highly sophisticated, designed to avoid detection for as long as possible.[40]

C. Flexible Regulatory Frameworks Enable Tailored Cybersecurity Practices

To date, leading cybersecurity frameworks, including the NIST Cybersecurity Framework ("CSF"), have wisely avoided prescriptive "one-size-fits-all approach[es]" to cybersecurity governance.[41] Instead, they have offered CISOs frameworks to prioritize vulnerabilities and triage risk. Amici know from their own experiences that a flexible approach to cybersecurity is required to distinguish between acceptable and unacceptable 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.

1. The NIST CSF

The federal NIST CSF is a leading framework, followed voluntarily by many public and private organizations.[42] The CSF recognizes that each organization has "different threats . . . vulnerabilities, [and] . . . risk tolerances," and that there is no "one-size-fits-all approach to

---

[38] FireEye, *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*, MANDIANT BLOG (Nov. 29, 2023), https://bit.ly/3Trst3z.

[39] *Analysis Report: MAR-10318845-1.v1—SUNBURST*, *supra* note 32.

[40] For a more comprehensive explanation of the novel and sophisticated SUNBURST attack, see Eckels, *supra* note 36; *Analysis Report: MAR-10318845-1.v1—SUNBURST*, *supra* note 32.

[41] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST 2 (Apr. 16, 2018), https://bit.ly/3vQqXPr (hereinafter "NIST CSF").

[42] *See* Federal Information Security Management Act ("FISMA"), 44 U.S.C. § 3541 *et seq*.

managing cybersecurity risk for critical infrastructure."[43] The CSF gives utmost flexibility to CISOs based on their distinct organizational needs and constraints. In fact, last month NIST released a comprehensive update to the CSF, which makes clear that the framework "describes what desirable outcomes an organization can *aspire* to achieve," but "does not *prescribe* outcomes."[44]

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 if they identify vulnerabilities through self-assessments under "the NIST Cybersecurity Framework"[45]—makes no sense.[46] Indeed, the SEC's attempt to effectively penalize an organization and its CISO for supposedly negative findings in NIST self-assessments undermines the CSF's key objective to "support self-assessment of investment effectiveness and cybersecurity activities."[47] 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."[48] In other words, routine self-monitoring confirms a company's good-faith attempt to implement the CSF and iteratively build cyber resilience. Here, 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.

---

[43] *See* NIST CSF, *supra* note 41, at 2.

[44] *Cybersecurity Framework Version 2.0*, NIST 1 (Feb. 26, 2024), https://bit.ly/3PcHFiS (first emphasis added).

[45] AC ¶ 72.

[46] *See* ECF No. 89 at 23.

[47] NIST CSF, *supra* note 41, at 20–21.

[48] *Id.* at 20.

2. The SEC's Cybersecurity Disclosure Rule

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."[49] 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 registrant has a [CISO] or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart."[50] Instead, the final rule now avoids "inadvertently pressur[ing] registrants to adopt specific or inflexible cybersecurity-risk governance practices or organizational structures."[51] These changes underscore that federal and state agencies, including the SEC, have deliberately abstained from establishing a prescriptive set of rules for cybersecurity governance.

D. 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.[52] As a result, on top of their internal duties, CISOs must engage with the broader cybersecurity ecosystem in which their

[49] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51,896 (Aug. 8, 2023) (to be codified at 17 C.F.R. pts. 22, 232, 240 & 249).

[50] *See id.* at 51,913–14.

[51] *See id.* at 51,915.

[52] *See, e.g.*, *Nonprofit Service Provider Blackbaud Settles Data Breach Case for $49.5M with States*, ASSOC. 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).

organizations are enmeshed. And because the private sector operates the vast majority of IT 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.[53] As CISA director Jen Easterly put it, "cyber[security] is a team sport."[54]

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."[55] 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."[56] As detailed below, *see* Section II.C *infra*, the SEC's claims could chill this critical cooperation, as CISOs would need to weigh whether voluntarily and proactively disclosing a vulnerability or breach to Government partners before public disclosure could increase their risk of personal liability.

---

[53] 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.

[54] Statement of Jen Easterly, *supra* note 2, at 2.

[55] Allen D. Householder et al., *The CERT Guide to Coordinated Vulnerability Disclosure*, CARNEGIE MELLON UNIV. SOFTWARE ENG'G INST. 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.

[56] *See* CISA, *Coordinated Vulnerability Disclosure Process*, https://bit.ly/42e108v (last visited Mar. 26, 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 providing insufficient detail about vulnerabilities in SolarWinds' information system in SEC filings. *See* AC ¶ 298 (implying that, to avoid liability, SolarWinds should have "disclose[d] the numerous risks, vulnerabilities, and incidents affecting its products in its SEC filings"). But, because of their responsibilities, CISOs engage with countless, novel "risks" and "vulnerabilities" daily. For 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.[57] These findings take time to fix due to technical complexity and resource constraints, and remain open issues in the meantime. As another example, organizations often use third-party software, in which its manufacturers discover risks and offer patches, which take time to implement across organizations.[58]

These are only a few 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 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 thousands, of ongoing vulnerabilities that they are working to mitigate in real-time. And as soon as one set of risks is resolved, others are virtually certain to arise because the vulnerability landscape is

[57] *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).

[58] For example, in 2023 alone, almost 29,000 such vulnerabilities were publicly reported by software companies through what is known as the CVE Program. *See* CVE, *Metrics: CVE Records*, https://bit.ly/42sl8ne (last visited Mar. 26, 2024). As another example, organizations commonly conduct "penetration testing" to probe their systems for weaknesses, which virtually always result in some findings of risks and vulnerabilities.

continuously changing and requires constant internal reassessment and scaffolding of risks, based on tradeoffs, priorities, and other constraints. Real-time disclosure of such risks, as the SEC's charges appear to advocate, would necessitate daily filings that "bury the shareholders in internal details . . . [that] fall[] outside the securities laws."[59]

Requiring organizations to provide detailed public disclosures of vulnerabilities would also result in harmful impacts 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 harm the cloud company and all others whose data the company hosts. As even the SEC has previously recognized, publicizing such information would be impractical, dangerous, and a radical departure from best practice.[60]

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."[61] Despite this recommendation by the Government's main cybersecurity agency and the SEC's own prior guidance, the SEC's theory of liability here would incentivize CISOs and companies to make premature and detailed disclosures

[59] *In re N. Telecom Ltd. Sec. Litig.*, 116 F. Supp. 2d 446, 459 (S.D.N.Y. 2000) (cleaned up). Contrary to the SEC's litigating position, the securities laws simply require disclosures "sufficient to pick up the . . . risk that later materialized." *Garnett v. RLX Tech. Inc.*, 632 F. Supp. 3d 574, 602 (S.D.N.Y. 2022) (Engelmayer, J.); *In re Qudian Inc. Sec. Litig.*, 2019 WL 4735376, at *8 (S.D.N.Y. Sept. 27, 2019) (finding disclosure that "security measures could be breached," the company "*may be unable . . . to implement adequate preventative measures*" against cyberattacks, and the company "*could be adversely affected*" by such an attack sufficient).

[60] SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Rel. Nos. 33-10459 & 34-82746, at 11 (Feb. 26, 2018), https://bit.ly/4cEwysQ ("We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident.").

[61] *Coordinated Vulnerability Disclosure Process*, *supra* note 56; *see also* ISO/IEC 30111, *supra* note 55; ISO/IEO 29147, *supra* note 55; Householder, *supra* note 55.

before root causes have been identified and mitigation strategies have been developed and carried out—all 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 *after discovery of* cyberattack also diverges from Government-endorsed best practices. *See* AC ¶¶ 312–14 (criticizing SolarWinds for stating it was "still investigating" certain issues rather than disclosing Mr. Brown's alleged preliminary suspicions about those issues). 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."[62] 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.[63]

DOJ's Best Practices for Cyber Victims recommends cyberattack victims take steps to "minimize continuing damage."[64] 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."[65] The FBI Director echoed those sentiments,

---

[62] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 27, at 2.

[63] *Id.* at 14.

[64] *Id.* at 7.

[65] 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) (statement of Rep. Yvette D. Clarke), https://bit.ly/3vOTaGh.

testifying that, during "cyber incidents [such as] SolarWinds," the Government should speak with "one voice" and not impose contradictory reporting requirements.[66]

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 had already formed a belief about that issue. *See, e.g.*, AC ¶¶ 312–14. The SEC's allegations disregard 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.[67] 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***."[68]

---

[66] Statement of Christopher A. Wray, *supra* note 20, at 7.

[67] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 27, at 12.

[68] *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").

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."[69] 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 "actively monitor defensive response measures and shift their methods to evade detection and containment,"[70] 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* AC ¶¶ 148–73, 178–213 (contrasting SolarWinds' policies on access controls, strong passwords, network monitoring, 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. It also risks transforming each preliminary cybersecurity assessment into a potential securities violation. 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

[69] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 27, at 13.

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

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. To the contrary, they would expect that a company's CISO would proactively identify areas for improvement. But under the SEC's approach, an assessment identifying a potential risk for remediation could provide a later basis for liability. Counterproductively, the SEC's charges incentivize information security employees to withhold tentative assessments out of fear that their identification of risks would later lead to liability, even if overstated or incorrect. Cybersecurity professionals should not have to consult lawyers before sending an email.

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. CISOs must advocate for investments in cybersecurity programs, including by pointing out deficiencies, to make their companies more secure. 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 understood, the severity of [the] risks" identified in those briefings. AC ¶ 198. 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 has already 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 would 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 CSF—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. AC ¶¶ 79–102 (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 his 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. AC ¶¶ 9–11, 117 (alleging that SolarWinds' 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.[71] AC ¶¶ 9–11, 97–101, 117–19, 128, 149–218, 305–31. 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.[72] The International Information System Security Certification Consortium ("ISC2") estimates a gap of 4 million globally and 482,985 in the United States.[73] 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.[74]

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,

---

[71] 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. & EXCH. COMM'N (Oct. 24, 2023), https://bit.ly/484SdqV.

[72] U.S. Dep't Defense, Directive No. 8000.01, Management of the Department 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." NAT'L INITIATIVE FOR CYBERSEC. EDUC., *Implementation Plan for the National Initiative for Cybersecurity Education Strategic Plan*, NIST 9 (2021), https://bit.ly/3HADTeR.

[73] *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.

[74] *See* Cambrie Eckert, *Just In: U.S. Desperately Needs Cyber Talent, Congress Says*, NAT'L DEF. MAG. 50 (June 26, 2023), https://bit.ly/3vWnKxw.

let alone one as technically demanding and dynamic as cybersecurity."[75] Over 40% of cybersecurity professionals report that their organizations face difficulties in hiring and retaining individuals with the necessary skills.[76] This workforce gap helps explain why most cybersecurity professionals believe their organizations are at "extreme" or "moderate risk" of a cyberattack.[77]

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,[78] including 19% (94) of Fortune 500 companies.[79] Organizations hiring across all industries face a severe lack of CISO candidates.[80] Without a qualified CISO on staff, organizations face near insurmountable hurdles in managing sophisticated cyberattacks.

Apart from hiring, organizations also struggle to retain their existing CISOs. Surveys show that average CISO tenure is less than five years.[81] 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.[82]

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

---

[75] *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 (2023) (statement of Will Markow, V.P. Applied Research, Advocacy, Glob. Mkts., Lightcast), https://bit.ly/4cACWl8.

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

[77] *Id.* at 26.

[78] *45% of Companies Do Not Employ a CISO*, SEC. MAG. (Nov. 24, 2021), https://bit.ly/3HRQUkt.

[79] Tim Howard, *The 2023 Fortune 500 CISOs Analysis*, FORTIFY EXPERTS BLOG (Nov. 17, 2023), https://bit.ly/48NQI1f.

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

[81] Matt Aiello et al., *2022 Global Chief Information Security Officer (CISO) Survey* 5, HEIDRICK & STRUGGLES 5 (2022), https://bit.ly/3SboRRE.

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

for a breach," and "job loss as a result of a breach."[83] Approximately 25% of CISOs expect to leave the CISO role entirely due to these overlapping "work-related stressors."[84]

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.[85]

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.[86]

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.[87]

---

[83] Aiello, *supra* note 81, at 12; *Growing the National Cybersecurity Talent Pipeline*, *supra* note 63, at 3 (statement of Rep. Andrew R. 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").

[84] GARTNER, *supra* note 82.

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

[86] *Cf.* Deepti Gopal et al., *Predicts 2023: Cybersecurity Industry Focuses on the Human Deal*, GARTNER 61 (Jan. 25, 2023), https://bit.ly/49rY2iS (noting that employee "churn will damage the [cybersecurity] mission and cost more").

[87] Statement of Christopher A. Wray, *supra* note 20, at 7.

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."[88]

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."[89] 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."[90]

The law should create incentives for cybersecurity professionals to voluntarily disclose to law enforcement known vulnerabilities, attempted cyberattacks and successful breaches. But knowing that they may be unfairly and disproportionately exposed to personal liability rather than treated as a victim could deter CISOs from creating the kind of "trusted relationship" with the Government that is essential to protect against cyberattacks. The SEC's claims here could make CISOs think twice before handing over 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.

---

[88] 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 § 106, 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).

[89] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 27, at 5.

[90] David Laufman et al., *Cyber Incidents: How Best to Work with Law Enforcement*, 1 CYBER SEC. 102, 103 (2017), https://bit.ly/3OjzOiR.

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.

March 29, 2024

Respectfully submitted,

/s/ *Andrew D. Goldstein*

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

Timothy T. Howard (4333233)
Robert Barton (5862545)
Susannah Benjamin (5924402)
FRESHFIELDS BRUCKHAUS DERINGER US LLP
3 World Trade Center, 175 Greenwich Street
New York, NY 10007
Phone: (212) 277-4000
Email: timothy.howard@freshfields.com
robert.barton@freshfields.com
susannah.benjamin@freshfields.com

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:

Brush Cyber, founded in 2017 and based in Denver, CO, is an international consulting firm specializing in dispute consulting, cybersecurity, and data governance. The firm offers a comprehensive approach to security and compliance and supports developing programs, closing critical gaps, and implementing necessary controls to meet regulatory requirements and enhance clients' security and privacy posture.

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 advancement of early stage and emerging growth cybersecurity companies into global markets. Its model connects cybersecurity, CISOs, risk executives, and professionals from venture capital, investment banking, system integration, policy, law, 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:[91]

- **Chirag Arora**, former CISO, Crum & Forster; Chair, GlobalCISO Leadership Foundation Advisory Board
- **James Azar**, CISO, AP4 Group
- **Michael Baader**, VP Cyber and Divisional CISO, Capital One
- **David Beabout**, Global CISO
- **Gerald Beuchelt**, CISO, Sprinklr Inc.; former CISO, LogMeIn; former CISO, Demandware
- **Louis Bobelis**, Deputy CISO and Head of Security Operations, AXIS Capital
- **Amy Bogac**, former CISO, The Clorox Company

[91] 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.

- **Sandy Buchanan**, Managing Director and former Chief Security Officer, Mirai Security, Inc.
- **Joanna Burkey**, former CISO, HP Inc.; former CISO, Siemens Americas
- **James Carder**, CISO, Eptura; former CISO, LogRhythm; Strategic Advisor and Founder, Cardiant Security, LLC
- **Aimee Cardwell**, former CISO, UnitedHealth Group
- **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
- **Eric Friedberg**, President and Founder, Next Tier Cybersecurity; former President, Stroz Friedberg
- **Oliver Friedrichs**, CEO, Pangea, former CEO, Phantom
- **Parrish Gunnels**, SVP and CISO
- **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
- **Patrick Heim**, Partner, SYN Ventures; Partner, ClearSky; former CISO
- **Ali Khan**, Field CISO, former CTO, and Advisor

- **Boris Kogan**, CISO, Interactive Brokers
- **David Lackey**, CISO, World Vision USA
- **Jay Leek**, former CISO, The Blackstone Group; Managing Partner, SYN Ventures
- **Larry Letow**, CEO, US, CyberCX
- **David Lin**, CISO, GIA
- **Siobhan MacDermott**, former CISO, Utilidata; former Principal, EY; former Head of Cyber Public Policy, Bank of America
- **Jon Miller**, CEO, Halcyon
- **Pritam Mungse**, Director of Product Security
- **Izak Mutlu**, former CISO, Salesforce, Inc.
- **Aaron Nasi**, Senior Director of Cybersecurity, Albertsons Companies
- **John Petrie**, former CISO, NTT Security Inc.; former CISO, Harland Clarke Holdings Corp.; former CISO, The University of Texas Health Science Center at San Antonio
- **Brandon Pinzon**, Chief Security Officer, Financial Services Industry
- **Robert Potter**, SYN Ventures
- **Michael Rosen**, Strategic Advisor, NightDragon
- **Andrew Smeaton**, former CISO, DataRobot, Inc.
- **Seth Spergel**, Managing Partner, Merlin Ventures
- **Eric Staffin**, former CISO, IHS Markit
- **Mike Stango**, Executive Director, Security50
- **Andrew Stone**, CTO and former CISO
- **Brett Wahlin**, former CISO, Activision Blizzard; former CISO, Amazon Prime Video; former CISO, Staples; former CISO, Hewlett-Packard

- **Larry Whiteside, Jr.**, CISO, RegScale; Co-Founder & President Emeritus, Cyversity
- **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
- **Shinichi Yokohama**, Group CISO, NTT Corporation
- **Brandon Young**, CISO, Republic Services; former CISO, Avnet
- **Sounil Yu**, CTO, Knostic; former CISO, JupiterOne; former Chief Security Scientist, Bank of America

CERTIFICATE OF SERVICE

I hereby certify that on March 29, 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