UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	No. 23-cv-9518 (PAE)

BRIEF OF *AMICI CURIAE* FORMER GOVERNMENT OFFICIALS

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, NW
Washington, DC 20006-1047
(202) 223-7300

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Statutes

Other Authorities

INTEREST OF AMICI

Amici curiae are over twenty former federal law enforcement and national security officials with expertise in cybersecurity. *Amici* have served in senior leadership roles in the federal government in which they participated in the highest levels of policy deliberations on cybersecurity. Collectively, *Amici* have devoted many years to protecting the national security interests of the United States spanning multiple administrations of both parties. *Amici* include the first National Cyber Director for the United States; the top Judge Advocate for the U.S. Cyber Command; the lead cyber official for the Department of Homeland Security; General Counsel of the National Security Agency and the highest-ranking civilian in the National Security Agency; the top national security lawyer for the Department of Justice; key Federal Bureau of Intelligence officials including the Chief of Staff and Senior Counsel to the Director, as well as Chief of Cyber Policy; a National Security Lawyer to the Central Intelligence Agency; and Chief of the Securities and Exchange Commission Office of Internet Enforcement.

Amici have an interest in ensuring that the Court is informed regarding the federal government's efforts to encourage private companies to share cybersecurity information with government authorities, including law enforcement and national security agencies, on a voluntary basis, as well as the risk that enforcement actions could disincentivize public-private information-sharing that is critically important to our nation's security.

The *Amici* are:

Stewart Baker served as a member of the Homeland Security Advisory Council from 2018 to 2021, as well as Assistant Secretary for Policy in the Department of Homeland Security from 2005 to 2009. Prior to that, he served as General Counsel of the National Security Agency from 1992 to 1994.

Austin Berglas served as Assistant Special Agent in Charge – Cyber in the Federal Bureau of Investigation from 1999 to 2015.

John P. Carlin served in the U.S. Department of Justice in multiple senior roles including as the Acting Deputy Attorney General and as the Assistant Attorney General for National Security. He also served in career roles as the National Coordinator of the Computer Hacking and Intellectual Property Program and as the Chief of Staff and Senior Counsel to the Director of the Federal Bureau of Intelligence.

Gus Coldebella served at the Department of Homeland Security as Acting General Counsel from 2007 to 2009, as well as Deputy General Counsel from 2005 to 2007.

Gary P. Corn has served as a Senior Fellow in the Army Cyber Institute from 2022 to present. Prior to that, he served as a Staff Judge Advocate in the U.S. Cyber Command from 2014 to 2019.

H. Bryan Cunningham served as Deputy Legal Adviser in the White House National Security Council from 2002 to 2004. Prior to that, he served as a Career CIA Officer and National Security Lawyer in the Central Intelligence Agency.

J. Michael Daniel served as Special Assistant to the President and Cybersecurity Coordinator in the Executive Office of the President from 2012 to 2017.

Jeff Greene served as Chief of Cyber Response and Policy in the White House National Security Council from 2021 to 2022. Prior to that, he served as Director of the National Cybersecurity Center of Excellence in the National Institute of Standards and Technology ("NIST") from 2020 to 2021, and as a member of the NIST Internet Security and Privacy Advisory Board from 2015 to 2020.

Melinda Haag served in the U.S. Department of Justice as United States Attorney for the Northern District of California from 2010 to 2015.

Chris Inglis served as National Cyber Director in the White House from 2021 to 2023. Prior to that, he served as Deputy Director of the National Security Agency from 2006 to 2014.

Steven M. Kelly served as Special Assistant to the President and Senior Director for Cybersecurity and Emerging Technology in the White House, National Security Council ("NSC") staff from 2022 to 2023. Both during and prior to that role, he served as a career Special Agent with the Federal Bureau of Investigation ("FBI") since 2002, was first seconded to the NSC's cybersecurity directorate from 2015 to 2017, and served as the FBI's Chief of Cyber Policy from 2017 to 2022.

Chris Krebs served as Director of the Cybersecurity and Infrastructure Security Agency from 2018 to 2020. Prior to that, he served in the Department of Homeland Security as the Under Secretary for the National Protection and Programs Directorate in 2018, as well as Assistant Secretary for Infrastructure Protection from 2017 to 2018.

James A. Lewis currently serves as a Distinguished Visiting Professor of Cyber Studies at the U.S. Naval Academy.

Joseph Moreno served as a Staff Member to the 9/11 Review Commission in the Federal Bureau of Investigation in 2014. Prior to that, he served in the U.S. Department of Justice as a Trial Attorney in the National Security Division.

Jeannie S. Rhee served in the U.S. Department of Justice as Assistant Special Counsel to Robert S. Mueller from 2017 to 2019, and Deputy Assistant Attorney General from 2009 to 2011.

Paul Rosenzweig served as Deputy Assistant Secretary for Policy in the U.S. Department of Homeland Security from 2005 to 2009.

Kurt Sanger, Lieutenant Colonel, U.S. Marine Corps (Ret.), served as an attorney for U.S. Cyber Command from 2014 to 2022, finishing as Deputy General Counsel of the Command.

Suzanne Spaulding served as Commissioner of the U.S. Cyberspace Solarium Commission from 2019 to 2020. Prior to that, she served as Under Secretary for the National Protection and Programs Directorate in the U.S. Department of Homeland Security from 2014 to 2017.

John Reed Stark served in the Securities and Exchange Commission (SEC) as the Chief of the SEC Office of Internet Enforcement from 1998 to 2009 and as "Special Counsel for Internet Projects" from 1994 to 1998.

Kemba Walden served as a Member of the Cyber Safety Review Board in the Department of Homeland Security from 2023 to 2024, as well as Acting National Cyber Director in the White House in 2023. Previous to that, she served as Principal Deputy National Cyber Director of the Office of the National Cyber Director from 2022 to 2023, and a Cybersecurity Attorney-Advisor in the U.S. Department of Homeland Security from 2016 to 2019.

Mark Weatherford served as Deputy Under Secretary for Cybersecurity in the Department of Homeland Security from 2011 to 2013.

ARGUMENT

I. CYBERATTACKS AGAINST PRIVATE AND PUBLIC SECTOR ENTITIES ARE A SERIOUS AND GROWING THREAT TO U.S. NATIONAL SECURITY.

Cyberattacks are a mounting threat to our national security. As the nation's economy and infrastructure have become more dependent on cyberspace, there has been a proliferation of threat actors seeking to exploit the vulnerabilities of our interconnected society, disrupt our critical infrastructure, steal and extort billions of dollars from American victims, steal our intellectual property, carry out malign influence operations, and engage in espionage and other criminal

activity.[1] Many threat actors, such as the prominent ransomware hacking group known as APT 41, receive financial and material support from foreign governments.[2] Some cyberattacks, including the attack that is the subject of this case, are perpetrated directly by elements of foreign governments.[3] This nation-state support permits dangerous actors to mount cyberattacks of unprecedented scale. In our experience, this means that not even the most sophisticated cybersecurity defenses, public or private, can reliably protect an information system from a dedicated, sophisticated threat actor.[4] This includes the systems of the United States government,

---

[1] *See, e.g.*, Fin. Crimes Enf't Network, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021* (Nov. 1, 2022), http://tinyurl.com/2s3tpvn6.

[2] Off. of Info. Sec. & Health Sector Cybersecurity Coordination Ctr., *APT41 and Recent Activity* (Sept. 22, 2022), http://tinyurl.com/9c5778wc. APT41 is an example of an Advanced Persistent Threat ("APT"), defined by the National Institute of Standards and Technology as "[a]n adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors" to "pursue[] its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives," which are typically to "exfilitrat[e] information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future." Nat'l Inst. of Standards & Tech., *Guide for Conduct Risk Assessments*, SP 800-30 Rev. 1 (Sept. 2012), http://tinyurl.com/2u6tx67t.

[3] *See, e.g.*, The White House, *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government* (Apr. 15, 2021), http://tinyurl.com/4tmmdtp8 ("[T]he United States is formally naming the Russian Foreign Intelligence Service (SVR), also known as APT 29, Coz Bear, and The Dukes, as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures."); Joe Uchill, *White House Confirms NotPetya Malware Was Russian Military Operation*, Axios (Feb. 15, 2018), http://tinyurl.com/5xkea2f5; William Turton & Jordan Robertson, *Microsoft Attack Blamed on China Morphs into Global Crisis*, Bloomberg (Mar. 8, 2021), http://tinyurl.com/y52j9y26.

[4] In a March 2021 speech, Department of Homeland Security Secretary Alejandro Mayorkas acknowledged the "hard truth is that no one is immune from cyber attacks, including the federal government or our most advanced technology companies." Dep't of Homeland Sec., *Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience* (Mar. 31, 2021), http://tinyurl.com/mv87trab.

with the Office of Personnel Management,[5] Department of Justice ("DOJ"),[6] Securities and Exchange Commission,[7] and even the National Security Agency[8] among the numerous federal agencies that have been victims of cyberattacks in the past decade.

II. COLLABORATION AND INFORMATION-SHARING BETWEEN THE PRIVATE SECTOR AND LAW ENFORCEMENT ARE CRITICAL TO COMBATING CYBERATTACKS.

The federal government has responded to this threat by prioritizing policies to support victims of cyberattacks and disrupt threat actors' ability to operate.[9] A key aspect of the federal government's defense against emerging cyber threats is close cooperation and information-sharing with the private sector. It is valuable for private entities to share information not only with peers,

---

[5] Off. of Pers. Mgmt., *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), http://tinyurl.com/47jke594.

[6] Dep't of Just., *Department of Justice Statement on Solarwinds Update* (Jan. 6, 2021), http://tinyurl.com/262bxcrb.

[7] Douglas Gillison, *US SEC Blames "SIM Swapping" for Its X Account Hack*, Reuters (Jan. 22, 2024), http://tinyurl.com/mprxb544.

[8] Nicole Perlroth & David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, N.Y. Times (May 12, 2017), http://tinyurl.com/4k939bd9.

[9] In its 2022-2026 Strategic Plan, for example, DOJ recognized the combat of ransomware attacks as an agency priority and the prosecution of cyber threat actors as an essential part of the federal government's "all tools approach" to combatting cybercrime. Dep't of Just., *FYs 2022-2026 Strategic Plan* (July 1, 2022), http://tinyurl.com/mpdxm97c; Off. of Pub. Affs., Dep't of Just., *Deputy Attorney General Lisa Monaco Delivers Remarks at American Bar Association National Institute on White Collar Crime* (Mar. 2, 2023), http://tinyurl.com/bdhaewpb. In 2023, the White House published a National Cybersecurity Strategy that names disruption and dismantling threat actors as a central element. The White House, *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy* (Mar. 2, 2023), http://tinyurl.com/38epzmzv. It also convened the International Counter Ransomware Initiative for a third gathering, bringing together enforcement agencies from 48 countries, the European Union, and Interpol to make commitments to share information, collaborate in response to cyber incidents, and refuse to pay ransoms to cyberattackers. The White House, *International Counter Ransomware Initiative 2023 Joint Statement* (Nov. 1, 2023), http://tinyurl.com/2yuvsm7z. Similarly, in 2022 Congress established the Joint Ransomware Task Force, an interagency body co-chaired by the FBI and Cybersecurity Infrastructure & Security Agency, to coordinate interagency efforts to combat ransomware and identify new initiatives to leverage the public and private sectors to defend against future attacks. Cybersecurity & Infrastructure Sec. Agency, *Readout of Second Joint Ransomware Task Force Meeting* (Dec. 14, 2022), http://tinyurl.com/2x37smdk.

through industry-centered Information Sharing and Analysis Centers ("ISACs"),[10] but also with law enforcement and national security agencies. These authorities are uniquely poised to respond to cyberattacks—sometimes, even ahead of the private victims. They have "tools and legal authorities that are unavailable to private entities."[11] Moreover, government agencies are positioned to identify larger trends in cybersecurity that would not otherwise be visible if kept to each individual private entity.[12]

Recent high-profile cyber incidents have demonstrated the important role law enforcement can play to assist victim companies and leverage the information they learn from victims to protect potential future victims. When infiltrating the Hive ransomware group's operations, for example, the FBI was able to leverage its access to threat actor servers to provide ransomware victims with decryption keys, and even warn some potential victims of the indicators of compromise before they were victimized.[13] An FBI official observed that information from victims is key: it permits the FBI to help victims and identify mistakes made by threat actors that would inform improved

[10] *See generally* Nat'l Council of ISACs, *About ISACs*, http://tinyurl.com/mutyjmdb (last visited Feb. 2, 2024) ("Information Sharing and Analysis Centers (ISACs) help critical infrastructure owners and operators protect their facilities, personnel[,] and customers from cyber and physical security threats and other hazards. ISACs collect, analyze[,] and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. The concept of ISACs was introduced and promulgated pursuant to Presidential Decision Direction-63 (PDD-63), signed May 22, 1998, after which the federal government asked each critical infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities.").

[11] Dep't of Just., *Best Practices for Victim Response and Reporting of Cyber Incidents* 19 (Sept. 2018), http://tinyurl.com/yh2x8mt7 [hereinafter DOJ Best Practices].

[12] *See* Cybersecurity & Infrastructure Sec. Agency, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 Fact Sheet* 2, http://tinyurl.com/txvvkjkt (last visited Feb. 2, 2024) ("When information about cyber incidents is shared quickly, we can use this information to render assistance and provide warning to prevent other organizations from falling victim to a similar incident.") [hereinafter CIRCIA Fact Sheet].

[13] Off. of Pub. Affs., Dep't of Just., *U.S. Department of Justice Disrupts Hive Ransomware Variant* (Jan. 26, 2023), http://tinyurl.com/8hx2fe7d.

future defenses.[14] In the wake of a cyberattack against Colonial Pipeline, as the company's CEO Joseph Blount testified to Congress, working closely with the FBI and Cybersecurity Infrastructure and Security Agency ("CISA") may have helped lead to the recovery of ransom funds.[15] Blount observed that, "[i]n combination with the government, we have a much better ability as Americans to thwart the threat of cyberattacks."[16] In response to cyberattacks perpetrated by the Blackcat group, the FBI was able to provide a decryption key to over 500 entities that may have otherwise been compelled to pay ransoms to recover data encrypted by the group.[17]

As these incidents above show, when government agencies are notified of a cyberattack on a private entity, they can take swift and effective action to respond. However, our experience has been that if victims do not come forward when they first learn of a cyber vulnerability or attack, public entities may not even know of the attack,[18] much less be able to take these concrete steps to respond.

Against this backdrop, many parts of the federal government responsible for national cybersecurity have encouraged victims of cyberattacks to promptly seek assistance from and share cyber information with the government.[19] In May 2021, President Biden issued an Executive

---

[14] Dina Temple-Raston & Gabriela Glueck, *Knocking Down Hive: How the FBI Ran Its Own Ransomware Decryption Operation*, THE RECORD (May 16, 2023), http://tinyurl.com/yeyus5r2.
[15] Brad D. Williams, *Pipeline CEO Defends Company's Cyber Info Sharing*, Breaking Def. (June 9, 2021), http://tinyurl.com/bdf58axm.
[16] *Id.*
[17] Off. of Public Affs., Dep't of Just., *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant* (Dec. 19, 2023), http://tinyurl.com/2kkrmfan.
[18] *See* Christopher Wray, *Remarks at the Detroit Economic Club: FBI Partnering with the Private Sector to Counter the Cyber Threat* (Mar. 22, 2022), http://tinyurl.com/42v7whnd ("If American businesses don't report attacks and intrusions, we don't know about most of them . . . .").
[19] *See, e.g.*, Dep't of Just., *Law Enforcement Cyber Incident Reporting: A Unified Message for State, Local, Tribal, and Territorial Law Enforcement*, http://tinyurl.com/5yph6x46 (last visited Feb. 2, 2024); *see also* Dep't of Homeland Sec., *National Cyber Incident Response Plan* 40-42 (Dec. 2016), http://tinyurl.com/wzzzzn72.

Order "prompted, in part, by the compromise of the SolarWinds software supply chain."[20] In it, he devoted an entire section to "[r]emoving barriers to sharing threat information."[21] CISA[22] and DOJ[23] have published best practices for cyber response that encourage private entities to share critical information about cyber incidents with those agencies. Individual government officials, too, have highlighted the need for the private and public sectors to come together. As President Biden stated, "the [f]ederal [g]overnment can't defend against [the cybersecurity] threat alone."[24] FBI Director Christopher Wray echoed the same message: "Because our adversaries rely on gaps in our community, they like it when we are not sharing information . . . ."[25] Reflecting on the attack on Colonial Pipeline, CISA Director Jen Easterly and CISA Cybersecurity Advisory Committee Chair Tom Fanning explained: "[R]ecognizing the need to bring together industry [and] government," the Joint Cyber Defense Collaborative was established "to catalyze a community of experts on the front lines of cyber defense—from across the public and private sectors—to share insights and information in real time."[26] FBI Assistant Director for the Cyber

[20] *See* Gov't Accountability Off., *Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746 at 20 (Jan. 13, 2022), http://tinyurl.com/2dutzda6.
[21] Exec. Order No. 14028, Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633, 26633-34 (May 12, 2021); *see also* The White House, *Statement by President Biden on our Nation's Cybersecurity* (Mar. 21, 2022), http://tinyurl.com/yp4ujc78 [hereinafter Biden Statement on Cybersecurity].
[22] CIRCIA Fact Sheet, *supra* note 1212.
[23] DOJ Best Practices, *supra* note 11, at 18.
[24] Biden Statement on Cybersecurity, *supra* note 21.
[25] Christopher Wray, *Director Wray Addresses CISA Cyber Security Summit*, Fed. Bureau of Intel. at 10:04-10:12 (Sept. 16, 2020), http://tinyurl.com/yc5s6vk2.
[26] Jen Easterly & Tom Fanning, *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years* (May 7, 2023), http://tinyurl.com/5f2wy99z.

Division Bryan Vorndran[27] and CISA Executive Assistant Director for Cybersecurity Eric Goldstein[28] have expressed similar sentiments.

Congress has also recognized the important role that information-sharing plays in the nation's cybersecurity response. It has enacted the Cybersecurity Information Sharing Act of 2015[29] and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA")[30] to encourage private entities to share information about cyber threats with the government. Both also underscore the importance of protecting companies that coordinate with the government from facing liability based on that information-sharing. The Cybersecurity Information Sharing Act was "designed to create a *voluntary* cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information, removing legal barriers and the threat of unnecessary litigation."[31] Concerned that the government could "inappropriately acquire or use sensitive information" for non-public safety purposes,[32] Congress included "narrowly tailored liability protection to incentivize" information-sharing.[33] In 2022, Congress also enacted CIRCIA, which authorizes CISA to promulgate regulations requiring public and private entities to

[27] Cybersecurity & Infrastructure Sec. Agency, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, http://tinyurl.com/9zfbjnrf (last visited Feb. 2, 2024) ("Developing a proactive relationship with your CISA regional cyber security advisor and local FBI field office . . . are necessary approaches to enable effective response and mitigation.").
[28] *Id.* ("Cyber risk is a shared challenge and we can't achieve success alone.").
[29] 6 U.S.C. § 1501 *et seq.*
[30] 6 U.S.C. § 681 *et seq.*
[31] S. Rep. No. 114-32 at 2 (Apr. 15, 2015) (emphasis in original).
[32] *Id.* at 3.
[33] *Id.*; *see also* 6 U.S.C. § 1505.

report cyber incidents and ransomware payments to the government.[34] CIRCIA, too, provides certain liability protections for companies that report cyber incidents.[35]

In our experience, such information-sharing and cooperation is most effective when information is shared quickly, often in the midst of a crisis when not all of the facts are known and information is likely to change. Even the shortest delay in sharing information can hamper the government's ability to effectively respond because threat actors can quickly delete evidence and move infrastructure before the government has an opportunity to seize or preserve the relevant evidence.[36] Additionally, when companies share cyber threat information in a confidential manner, it provides the government with the time to discreetly investigate an incident or vulnerability and take action—such as providing a decryption key, recovering stolen data, or gaining access to threat actor infrastructure—without tipping off the threat actors.[37] Indeed, the FBI and Secret Service "work with victim companies to avoid unwarranted disclosure of information . . . [and] will generally coordinate public statements concerning the incident with victim companies" precisely because they must "ensure that harmful or sensitive information is not needlessly disclosed."[38]

---

[34] 6 U.S.C. §§ 681b (companies required to report cyber incidents to CISA within 72 hours after they reasonably believes a cyber incident has occurred), 681c (companies encouraged to voluntarily report ransomware payments).
[35] 6 U.S.C. § 681e(c).
[36] *See* DOJ Best Practices, *supra* note 11, at 15-17 (highlighting, as part of incident response, the importance of "preserv[ing] a record of a server at the time of the incident").
[37] Temple-Raston & Glueck, *supra* note 14 (discussing how FBI decided whether to make decryption keys public to victims during its covert investigation of Hive while ensuring the "long-term pursuit of justice" and its operation).
[38] *See* DOJ Best Practices, *supra* note 1111, at 19; Dep't of Homeland Sec., *Harmonization of Cyber Incident Reporting to the Federal Government* 7 (Sept. 19, 2023), http://tinyurl.com/2vytyxwr ("The Federal Government should ensure that sensitive cyber incident information reported by the private sector is protected from disclosure . . . .").

III. WE URGE THE COURT TO CAREFULLY EVALUATE HOW ENFORCEMENT ACTIONS MAY DISINCENTIVIZE OR CHILL COMPANIES FROM SHARING CRITICAL CYBERSECURITY INFORMATION WITH THE GOVERNMENT.

We caution the Court that, in evaluating actions like this one, it is important to be cognizant of the risk of chilling voluntary disclosure by companies or CISOs, who may become more cautious when considering how their communications regarding cybersecurity threat information—whether directly with the government or with peers through ISACs[39]—might increase future liability. Public disclosure is not a substitute for, and must not come at the expense of, voluntary confidential sharing of more detailed cyber threat information with the agencies tasked with combatting cyber threats, who have the right set of technical tools and legal authority to take effective action. Moreover, a regime that incentivizes early detailed public disclosure of vulnerability information, along with information detailing a company's security posture, can actually damage law enforcement investigations, provide a roadmap to aid threat actors, and make companies less safe. Courts should evaluate actions like this one while keeping in mind the importance of avoiding action that might chill or otherwise disincentivize the important information-sharing and cooperation discussed in Section II.[40]

Cybersecurity risks are far easier to evaluate after a risk has already materialized and been eliminated. A CISO or company concerned that the preliminary information about a cybersecurity

[39] Under the Cybersecurity Information Sharing Act of 2015, "private entities that share a cyber threat indicator or defensive measure with an ISAC . . . receive liability protection and other protections and exemptions for such sharing." Dep't of Homeland Sec. & Dep't of Just., *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* 15 (Oct. 2020), http://tinyurl.com/3x5b8phw.

[40] *See* Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, Cong. Rsch. Serv. Rep. 7-5700, at 38-39 (Mar. 16, 2015) ("[A] fear exists that information disclosed by a company to the government as part of a cyber-information sharing arrangement . . . could be used as evidence to show that the company withheld material information from the SEC.").

incident or vulnerability it shares with law enforcement or industry may be treated in hindsight as something that should have been disclosed publicly may think twice before sharing that information in the first place. As it evaluates this action, we would therefore urge this Court to consider the importance of public-private sector sharing of cybersecurity threat information to the nation's ability to prevent and respond to cyberattacks.

Dated: Washington, DC
February 2, 2024

Respectfully submitted,

PAUL, WEISS, RIFKIND,
WHARTON & GARRISON LLP

By: */s/ John P. Carlin*
John P. Carlin (*pro hac vice* motion pending)

2001 K Street, NW
Washington, DC 20006-1047
(202) 223-7300
jcarlin@paulweiss.com

By: */s/ Jeannie S. Rhee*
Jeannie S. Rhee (*pro hac vice* motion pending)

2001 K Street, NW
Washington, DC 20006-1047
(202) 223-7300
jrhee@paulweiss.com

Counsel for Amici Curiae Former Government Officials