May 22, 2023

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

Re: File No. S7-04-22 Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

Dear Secretary Countryman:

In addition to regulation of securities market issuers, the Securities & Exchange Commission (SEC) is also responsible for regulation of those entities that provide the networks, either electronic or physical, that enable the functioning of our securities markets.[1] On February 9, 2022, the Commission published a Release for Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies containing proposals that, if adopted, would establish a new cybersecurity incident reporting and disclosure regime and require registered investment advisers ("advisers") and investment companies ("funds") to implement policies and procedures designed to address cyber risks.[2] The comment period for this proposed rule was reopened on March 15, 2023 as File No. S7-04-22. As a result, during March 2023, the SEC had several proposed rules relating to strengthening disclosures by certain market participants.[3] Because each of these proposed rules relate to the

[1] Neal Newman & Lawrence J. Trautman, *Securities Law: Overview and Contemporary Issues*, 16 OHIO ST. BUS. L.J. 149 (2021), http://ssrn.com/abstract=3790804.
[2] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release Nos. 33-11028, IA-5956, IC-34497, 87 Fed. Reg. 13524 (proposed Feb. 9, 2022) (to be codified at 17 C.F.R. pts. 230, 232, 239, 270, 274, 275, 279).
[3] *See also* Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Release No. 34-97141, IA-6262, IC-34854 (proposed Mar. 15, 2023); Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the

ongoing cybersecurity threat, our comments are applicable to each. One of these proposed rules requires "broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents (collectively, 'Market Entities') to address their cybersecurity risks."[4] SEC Chairman Gary Gensler states that "cybersecurity risks have grown significantly in recent decades. Investors, issuers, and market participants alike would benefit from knowing that these entities have in place protections fit for a digital age. This proposal would help promote every part of our mission, particularly regarding investor protection and orderly markets."[5]

This Comment proceeds in six parts. First, we demonstrate that the danger posed by cybersecurity threat continues at an alarming pace. Second, we elaborate to show that cyber threat endangers all segments of society due to the increasing technological connectivity of all parties. Third, we discuss the Commission's proposed new rules. Fourth, we look at some of the representative comments already received. Fifth, we register our support and thanks to Chairman Gensler and the staff for their hard work required to strengthen our nation's coordinated support for increased cybersecurity. And last, we conclude.

Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Release No. 34-97142 (proposed Mar. 15, 2023).

[4] PRESS RELEASE 2023-52, SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-52.
[5] PRESS RELEASE 2023-52, SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-52.

I. CYBER THREAT CONTINUES

Cyber attacks, including those mounted by nation states against American computers continue at an alarming rate.[6] With global markets increasingly interdependent and interconnected the Commission has previously observed, "as technological advancements and commercial developments have changed how our securities markets operate, our ability to remain an effective regulator requires us to continuously monitor the market environment and, as appropriate, adjust and modernize our expertise, rules, regulations, and oversight tools and activities."[7] The success or failure of our society, jobs of a global workplace, and the ability of families everywhere to feed, clothe, and house themselves depends on the success of the SEC in providing fair and open access to capital through efficient markets. Consider that, "The proliferation of novel consumer devices and increased Internet-dependent businesses and

---

[6] Annual Meeting Paper from Robert Axelrod, The Strategic Timing of Cyber Exploits, to American Political Science Association (Aug. 29–Sept. 1, 2013); Communist Chinese Cyber-Attacks, CyberEspionage and Theft of American Technology: Hearing Before the H. Subcomm. on Oversight and Investigations of the Comm. on Foreign Affairs, 112th Cong. 112–14 (2011); Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012); Eric Talbot Jensen, Cyber Warfare and Precautions Against the Effects of Attacks, 88 TEX. L. REV. 1533 (2010); Jay P. Kesan & Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 HARV. J.L. & TECH. 429 (2012); Asaf Lubin, *The Law and Politics of Ransomware*, 55 VAND. J. TRANS'L L.1177 (2022), https://ssrn.com/abstract=4181964; William J. Lynn, Defending a New Domain, 89 FOREIGN AFF. 97 (2010); Nathan Alexander Sales, Regulating Cyber-Security, 107 NW. U.L. REV. 1503 (2013); Anna D. Scherbina & Bernd Schlusche, The Effect of Malicious Cyber Activity on the U.S. Corporate Sector (March 25, 2023), https://ssrn.com/abstract=4400066; Scott Shackelford & Amanda Craig, Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity, 50 STAN. J. INT'L L. 119 (2014); Peter P. Swire, A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?, 2 J. TELECOMM. & HIGH TECH. L. 163 (2004); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J. L. TECH. & POL'Y 341 (2015), http://ssrn.com/abstract=2548561; Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works,* 5 J. L. & CYBER WARFARE 147 (2016), http://ssrn.com/abstract=2638448.

[7] *See* Newman & Trautman, *supra* note 1, *citing* What We Do, Maintaining Fair, Orderly and Efficient Markets, SEC, Sec.gov., https://www.sec.gov/about/what-we-do. *See also* Lawrence J. Trautman & Neal Newman, *A Proposed SEC Cyber Data Disclosure Advisory Commission,* 50 SEC. REG. L.J. 199 (2022), http://ssrn.com/abstract=4097138; Lawrence J. Trautman & George P. Michaely, *The SEC & The Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L.Q. RPT. 262 (2014), http://www.ssrn.com/abstract=1951148.

government data systems introduce vulnerabilities of unprecedented magnitude."[8] For example, as early as 2010, "Discovery of the industrial virus Stuxnet… introduced a global threat of malware focused toward disruption of industrial control devices."[9]

Clear and Present Danger

In a previously published law review article, one of your commentators has warned that:

> With the power to wreak havoc on global economic and political stability, cyber issues remain likely the greatest single threat to modern civilization. Now, just as in the days and weeks immediately preceding the 1941 attack against the United States at Pearl Harbor, all the necessary warning signs are there. Enemies have probed and fully mapped the data systems of America's important corporations and institutions. The future of the United States, represented by its intellectual property, has systematically been stolen by its adversaries. Initial sounding of the alarm, "the hackers are coming; the hackers are coming" may have already faded from deaf ears. However, beware, the hackers are here! The hackers are here![10]

The Wall Street Journal reports on May 17, 2023 that SEC Chairman Gary Gensler warn that "the next financial crisis could emerge from firm's use of artificial intelligence… warning of the potential 'systemic risk' posed by the technology's proliferation."[11] Additional remarks attributed to Chairman Gensler include that, "Data aggregators and AI platforms could be major components of future financial system 'fragility.'"[12] In addition:

> Observers years from now might look back and say 'the crisis in 2027 was because everything was relying on one base level, what's called [the] generative AI level, and a bunch of fintech apps are built on top of it… Banks and other financial institutions have employed AI in a variety of functions, including for the normally laborious compliance work involved in sizing up new customers or checking for

[8] Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018), http://ssrn.com/abstract=2982629.
[9] Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018), http://ssrn.com/abstract=2982629.
[10] Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?*, 18 N. C. J. L. & TECH. 232 (2016), http://ssrn.com/abstract=2711059.
[11] Richard Vanderford, *AI Could Spark Next Financial Crisis, SEC Chief Says*, Wall St. J., May 17, 2023 at B3.
[12] *Id.*

suspicious transactions. But despite the possible efficiency gains, the systems should be closely scrutinized.[13]

II. ALL SEGMENTS OF SOCIETY THREATENED

The technological changes brought about during the past two decades has resulted in new interconnectedness that introduces increased systematic risk to all societal institutions. For purposes of our securities markets, "Market Entities increasingly rely on information systems to perform their functions and provide their services and thus are targets for threat actors who may seek to disrupt their functions or gain access to the data stored on the information systems for financial gain."[14] In addition, "Cybersecurity risk also can be caused by the errors of employees, service providers, or business partners. The interconnectedness of Market Entities increases the risk that a significant cybersecurity incident can simultaneously impact multiple Market Entities causing systemic harm to the U.S. securities markets."[15] As shown during the 2008 U.S. mortgage meltdown, failure of our capital and securities markets quickly spills over into other international markets resulting in unemployment and widespread human suffering.[16] As recent as 2023, the bankruptcy of FTX and other crypto entities—along with the failure of Silicon Valley Bank and First Republic caused significant stress from deposit withdrawals among regional banks.[17]

---

[13] *Id. See also* Lawrence J. Trautman & W. Gregory Voss, The Evolution of Machine Learning, Artificial Intelligence, and Generative Pre-Trained Transformer (GPT) and Why Should We Care? (unpub. m.s.).
[14] PRESS RELEASE 2023-52, SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-52.
[15] PRESS RELEASE 2023-52, SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-52.
[16] Lawrence J. Trautman, Personal Ethics & the U.S. Financial Collapse of 2007-08: Decade Later After-Action Report, http://ssrn.com/abstract=2502124.
[17] Lawrence J. Trautman, The FTX Crypto Debacle: Largest Fraud Since Madoff?, __ U. MEMPHIS L. REV. (forthcoming), http://ssrn.com/abstract=4290093.

Struggle of Law to Keep Pace With Rapid Technological Change

Much like Moore's Law which predicts that, "computing power would double every two years—a forecast that has proved remarkably durable,"[18] technological change continues at a staggering rate. In the past two decades alone, the Internet has evolved to create significant privacy challenges,[19] blockchain technologies[20] have enabled new applications such as virtual currencies,[21] the Internet of Things (IoT) has resulted in billions of new vulnerabilities;[22] non-fungible tokens (NFTs),[23] and recently, artificial intelligence, machine learning and GPT have introduced new potential threat surfaces,[24] just to name a few. Rapid technological change creates novel issues for our intellectual property laws.[25] Technological advances may cause

[18] HENRY A. KISSENGER, ERIC SCHMIDT & DANIEL HUTTENLOCHER, THE AGE OF AI, 86 (Back Bay Books, 2021).
[19] Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-Commerce, Political and Regulatory Compliance Risks,* 10 WM. & MARY BUS. L. REV. 1 (2018), https://ssrn.com/abstract=3067298; Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis,* 20 PITTS. J. TECH. L. & POL'Y 41 (2020), http://ssrn.com/abstract=3363002.
[20] Michael J. Conklin, Brian Elzweig & Lawrence J. Trautman, Legal Recourse for Victims of Blockchain and Cyber Breach Attacks, 23 U.C. DAVIS BUS. L.J. (forthcoming 2022-2023), http://ssrn.com/abstract=4251666; Lawrence J. Trautman & Mason J. Molesky *A Primer for Blockchain,* 88 UMKC L. REV. 239 (2019), arXiv:1904.03254, https://ssrn.com/abstract=3324660; Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?,* 69 CONSUMER FIN. L. Q. RPT. 232 (2016), http://ssrn.com/abstract=2786186.
[21] Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?,* 20 RICH. J. L. & TECH. 13 (2014), http://www.ssrn.com/abstract=2393537; Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?,* 38 CARDOZO L. REV. 1041 (2017), http://ssrn.com/abstract=2730983; Lawrence J. Trautman, *Bitcoin, Virtual Currencies and the Struggle of Law and Regulation to Keep Pace,* 102 MARQ. L. REV. 447 (2018), https://ssrn.com/abstract=3182867.
[22] Mohammed T. Hussein & Lawrence J. Trautman, The Internet of Things (IoT) in a Post-Pandemic World, 9 JOURNAL OF LAW & CYBER WARFARE, (forthcoming), http://ssrn.com/abstract=4149477; Lawrence J. Trautman, Mohammed T. Hussein, Louis Ndamase & Mason Molesky *Governance of The Internet of Things (IoT),* 60 JURIMETRICS 315 (Spring 2020), http://ssrn.com/abstract=3443973.
[23] Brian Elzweig & Lawrence J. Trautman, When Does A Nonfungible Token (NFT) Become A Security?, 39 GA. ST. U. L. REV. 295 (2023), http://ssrn.com/abstract=4055585; Lawrence J. Trautman, *Virtual Art and Non-fungible Tokens,* 50 HOFSTRA L. REV. 361 (2022), http://ssrn.com/abstract=3814087.
[24] Lawrence J. Trautman & W. Gregory Voss, The Evolution of Machine Learning, Artificial Intelligence, and Generative Pre-Trained Transformer (GPT) and Why Should You Care? (unpub. m.s.).
[25] Timothy T. Hsieh, Robert W. Emerson, Larry D. Foster II, Brian A. Link, Cherie A. Sherman & Lawrence J. Trautman, Intellectual Property in the Era of AI, Blockchain, and Web 3.0, http://ssrn.com/abstract=4392895.

disruptive changes to employment.[26] Failures of virtual currency-related entities during 2022 and 2023 have caused major financial losses worldwide.[27] Some of these losses have spilled over into the traditional banking system resulting in the failures of crypto-lending Signature Bank in the United States,[28] and playing perhaps a lesser direct role in the fate of Silicon Valley Bank and others.[29]

While the proposed rule relate succinctly to potential cyber risk impacting covered Market Entities, it is important to consider the risks resulting from the interconnectedness of various societal institutions such as: corporate and other business entities; educational; federal, state, and municipal governments; healthcare; information technology infrastructure vendors; and the national security community.

Corporations and Other Business Entities

Few topics during recent years have demanded more attention from management and corporate boards than cybersecurity.[30] Courts have recently held that cybersecurity is a "mission

[26] Mohammed T. Hussein, Lawrence J. Trautman & Reginald Holloway, Technology Employment, Information and Communications in the Digital Age, 103 J. U.S. PATENT & TRADEMARK OFF, SOC., 101 (Jan. 2023), http://ssrn.com/abstract=3762273.
[27] Lawrence J. Trautman, The FTX Crypto Debacle: Largest Fraud Since Madoff?, __ U. MEMPHIS L. REV. (forthcoming), http://ssrn.com/abstract=4290093.
[28] Lawrence J. Trautman, The FTX Crypto Debacle: Largest Fraud Since Madoff?, __ U. MEMPHIS L. REV. (forthcoming), http://ssrn.com/abstract=4290093.
[29] Lawrence J. Trautman, The FTX Crypto Debacle: Largest Fraud Since Madoff?, __ U. MEMPHIS L. REV. (forthcoming), http://ssrn.com/abstract=4290093.
[30] Hon. Bernice Donald, Brian Elzweig, Neal F. Newman, H. Justin Pace & Lawrence J. Trautman, Crisis at the Audit Committee: Challenges of a Post-Pandemic World, REV. BANKING & FIN. L. [Boston University] (forthcoming), http://ssrn.com/abstract=4240080; David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability*, 18 COL. TECH. L.J. 49 (2020), http://ssrn.com/abstract=3251479; Lawrence J. Trautman, Scott Shackelford, Brian Elzweig & Peter C. Ormerod, Cyber Threats to Business: Identifying and Responding to Digital Attacks, (unpub. m.s.), https://ssrn.com/abstract=4262971; Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231 (2017), http://ssrn.com/abstract=2883607; Lawrence j. Trautman, *The Board's Responsibility for Crisis Governance,* 13 HASTINGS BUS. L.J. 275 (2017), http://ssrn.com/abstract=2623219; Lawrence J. Trautman, *E-Commerce, Cyber and Electronic Payment System Risks: Lessons from PayPal*, 16 U.C. DAVIS BUS. L.J. 261 (Spring 2016), http://www.ssrn.com/abstract=2314119; Lawrence J. Trautman, *Who Sits on Texas Corporate Boards?*

critical" responsibility for corporate boards.[31] As disclosed more fully later, seven U.S. Senators recommend that:

> One effective regulatory approach would be asking public companies to disclose whether a cybersecurity expert is on the board of directors, and if not, why not. We have sponsored bipartisan legislation called the Cybersecurity Disclosure Act to require companies to provide this disclosure to investors. The bill does not tell companies how to deal with cybersecurity threats. How a company chooses to address cybersecurity risks would remain its own decision. Boards of directors would be encouraged to develop approaches that address their own needs. The goal is to encourage directors to play a more effective role in cybersecurity risk oversight.[32]

Educational Institutions

Often plagued with outdated legacy IT systems and modest budgets for investments in infrastructure and talent, educational institutions have been ripe targets for both student hacking attempts and ransomware attacks.[33]

Texas Corporate Directors: Who They Are and What They Do, 16 HOUSTON BUS. & TAX L.J. 44 (2016), http://ssrn.com/abstract=2493569; Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?,* 11 DEPAUL BUS. & COMM. L.J. 205 (2013), http://www.ssrn.com/abstract=2137747; Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FLA. ST. U. BUS. REV. 75 (2012), http://www.ssrn.com/abstract=1998489.

[31] H. Justin Pace & Lawrence J. Trautman, *Mission Critical: Caremark. Blue Bell, and Director Responsibility for Cybersecurity Governance*, 2022 WISC. L. REV. 887 (2022), http://ssrn.com/abstract=3938128. *See also* H. Justin Pace & Lawrence J. Trautman, Financial Institution D&O Liability After Caremark and McDonald's (unpub. m.s.); Lawrence J. Trautman, Seletha Butler, Frederick R. Chang, Michele Hooper, Ron McCray & Ruth Simmons *Corporate Directors: Who They Are, What They Do, Cyber and Other Contemporary Challenges*, 70 BUFFALO L. REV. 459 (2022), http://ssrn.com/abstract=3792382.

[32] Letter from U.S. Senators Susan M. Collins, Kevin Cramer, Catherine Cortez Masto, Angus S. King, Jr., Jack Reed, Mark R. Warner, and Ron Wyden to Gary Gensler, Chairman, SEC (Feb. 8, 2022), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sec.gov/comments/s7-09-22/s70922-20127532-288660.pdf. *Infra* note __.

[33] Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018), http://ssrn.com/abstract=2982629. *See also* Lawrence J. Trautman & Janet Ford *Nonprofit Governance: The Basics*, 52 AKRON L. REV. 971 (2018), https://ssrn.com/abstract=3133818.

Federal, State, and Municipal Governments

Almost all governmental entities continue to be targets of cybersecurity attacks and ransomware exploits.[34] Elsewhere Trautman and Ormerod have reported that "during mid-March 2018 the city of Atlanta received a ransom demand from hackers known as The SamSam group, requesting a payment of about $51,000 to be made in Bitcoin.[35] In addition:

> *The New York Times* characterizes the Atlanta attack as, "one of the most sustained and consequential cyberattacks ever mounted against a major American city… [and] laid bare once again the vulnerabilities of governments as they rely on computer networks for day-to-day operations." While wastewater systems and the systems involving 911 emergency telephone calls were not impacted, "other arms of city government have been scrambled for days. The Atlanta Municipal Court has been unable to validate warrants. Police officers have been writing reports by hand. The city has stopped taking employment applications." Even after the desktop computers for roughly 8,000 Atlanta employees came "back to life for the first time in five days, residents still could not pay their traffic tickets or water bills online, or report potholes or graffiti on a city website. Travelers at the world's busiest airport still could not use the free Wi-Fi." It appears that victims often prefer to pay a ransom of $50,000 or so, than incur "the time and cost of restoring their locked data and compromised systems. In the past year, the group has taken to attacking hospitals, police departments and universities − targets with money but without the luxury of going off-line for days or weeks for restoration work. So, what appears to be the cost to Atlanta? Atlanta mayor Keisha Lance Bottoms, speaking in mid-2018 at a mayor's conference, "estimated that the city, which decided to rebuild its systems, was facing more than $20 million in costs, but she hoped insurance would cover much of that."[36]

[34] Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018), http://ssrn.com/abstract=2982629.
[35] *See* Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 536 (2019), http://ssrn.com/abstract=3238293.
citing Alan Blinder & Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder*, N.Y. TIMES, Mar. 27, 2018, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.
[36] *Id.* (internal citations omitted).

As we draft these comments, the city of Dallas is attempting to recover from a month-long (at this point) impactful ransomware attack attributed to a group known as The Royal Group[37]

Healthcare

Hospitals and other healthcare entities have been shown to be prime targets for cyber and ransomware attacks.[38] For example, Professor Deborah Farringer has observed that, "[w]hile hackers and data breaches are not new in the healthcare context, ransomware attacks are unique in the way they have a direct and immediate impact on the actual provision of care to patients and present a very real threat to patient safety."[39] In her excellent law review Article she writes, "[s]adly, the potential devastation that could be caused when hospitals and health systems lose access to their EHRs [Electronic Health Records] and computer systems is exactly what makes these types of attacks so attractive to potential hackers."[40] Because of the critical importance of hospitals and other parts of the healthcare system, we will briefly review several of these attacks:

> MedStar Health
> On March 28, 2016, MedStar Health, a ten hospital non-profit system operating in Washington, D.C., Virginia and Maryland received pop-up messages reading: "You have 10 days to send us the Bitcoin…[A]fter 10 days we will remove your private key and it's impossible to recover your files." A MedStar employee provided *The Washington Post* with a copy of the ransom note image, "which demanded that the $5billion health-care provider pay 45 bitcoins − equivalent to about $19,000 − in exchange for the digital key that would release the data. While the FBI investigated, the ransomware cyberattack, "forced MedStar's 10 hospitals and more than 250 outpatient centers to shut down their computers and email…"

---

[37] Carly Page, *Ransomware Attack Forces Dallas to Shut Down Courts, Disrupts some 911 Services,* Techcrunch.com (May 4, 2023), https://techcrunch.com/2023/05/04/ransomware-attack-forces-dallas-to-shut-down-courts-disrupt-some-911-services/.

[38] *See* Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations,* 86 TENN. L. REV. 503, 517 (2019), http://ssrn.com/abstract=3238293.
Citing Deborah Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals,* 40 SEATTLE U. L. REV. 937 (2017), https://ssrn.com/abstract=2995095.

[39] *Id.*

[40] *Id.*

> *The Washington Post* account reports learning from a nurse at the MedStart Washington Hospital Center that "Without access to email and computer systems, the medical staff fell back on seldom-used paper records that had to be faxed or hand delivered. But this nurse and another told The Post that the paper charts are far less comprehensive than those kept in digital form."
>
> Hollywood Presbyterian Medical Center, Los Angeles
>
> On February 5, 2016 hackers successfully employed malware to infect the computer system at Hollywood Presbyterian Medical Center, "preventing hospital staff from being able to communicate from those devices," according to CEO Allen Stefanek." The hackers demanded and Hollywood Presbyterian paid the equivalent of approximately $17,000, denominated in 40 bitcoin. CEO Stefanek stated, "The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key… In the best interest of restoring normal operations, we did this." The Los Angeles Times reported learning from law enforcement sources, "that the hospital paid the ransom before reaching out to law enforcement for assistance."[41]

National Security

Former CIA Director Leon Panetta has observed that, "the next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems."[42] As discussed previously, just one example of how developments in the nation state arena may threaten business entities and capital and securities markets consider how, "Discovery of the industrial virus Stuxnet… introduced a global threat of malware focused toward disruption of industrial control devices."[43]

---

[41] *Id.*

[42] Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?,* 18 N. C. J. L. & TECH. 232 (2016), http://ssrn.com/abstract=2711059. *See also* Lawrence J. Trautman, *Managing Cyberthreat,* 33(2) SANTA CLARA HIGH TECH. L.J. 230 (2016), http://ssrn.com/abstract=2534119.

[43] Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things,* 72 U. MIAMI L. REV. 761 (2018), http://ssrn.com/abstract=2982629.

III. THE PROPOSED NEW RULES

Several proposed new rules have been proposed during March 2023 to strengthen focus and responsibility for cybersecurity by various market participants.[44] We will now briefly present a summary of relevant provisions.

The Cybersecurity Risk Management Rules

During March 2023, the Commission issued proposed rules for comment intended to strengthen cybersecurity risk management. A summary of these proposed rule is described by the SEC as follows:

> The Commission is proposing new cybersecurity risk management rules and related amendments to certain rules under the Investment Advisers Act of 1940 (the "Advisers Act") and the Investment Company Act of 1940 (the "Investment Company Act"). The proposed rules and amendments would enhance cybersecurity preparedness and improve the resilience of investment advisers and investment companies against cybersecurity threats and attacks by:
>
> - Requiring advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks;
> - Having advisers report significant cybersecurity incidents to the Commission on proposed Form ADV-C;
> - Enhancing adviser and fund disclosures related to cybersecurity risks and incidents; and
> - Requiring advisers and fund to maintain, make, and retain certain cybersecurity-related books and records.
>
> Background
>
> Advisers and funds play an important role in our financial markets and increasingly depend on technology for critical business operations. Advisers and funds are exposed to, and rely on, a broad array of interconnected systems and networks, both directly and through service providers such as custodians, brokers, dealers, pricing services, and other technology vendors. As a result, they face numerous cybersecurity risks and may experience cybersecurity incidents that can cause, or be exacerbated by, critical system or process failures.
>
> The Commission is concerned about the efficacy of adviser and fund practices industry-wide to address cybersecurity risks and incidents, and that less

[44] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release Nos. 33-11028, IA-5956, IC-34497, 87 Fed. Reg. 13524 (proposed Feb. 9, 2022) (to be codified at 17 C.F.R. pts. 230, 232, 239, 270, 274, 275, 279).

robust cybersecurity practices may not adequately address investor protection concerns. There is also concern about the effectiveness of disclosures to advisory clients and fund shareholders concerning cybersecurity risks and incidents. The Commission's proposed rules and amendments are designed to address concerns about advisers' and funds' cybersecurity preparedness and reduce cybersecurity-related risks to clients and investors; to improve the disclosures clients and investors receive about advisers' and funds' cybersecurity exposures and the cybersecurity incidents that occur at advisers and funds; and to enhance the Commission's ability to assess systemic risks and its oversight of advisers and funds.

Proposed Amendments

Cybersecurity Risk Management Rules The proposal includes new rule 206(4)-9 under the Advisers Act and new rule 38a-2 under the Investment Company Act (collectively, the "proposed cybersecurity risk management rules'). The proposed cybersecurity risk management rules would require advisers and funds to adopt and implement policies and procedures that are reasonably designed to address cybersecurity risks. The proposed rules enumerate certain general elements that advisers and funds would be required to address in their cybersecurity policies and procedures. These policies and procedures would help address operational and other risks that could harm advisory clients and fund investors or lead to the unauthorized access to or use of adviser or fund information, including the personal information of their clients or investors.

Reporting of Significant Cybersecurity Incidents

The proposal also includes a reporting requirement under new rule 204-6 that would require advisers to report significant cybersecurity incidents to the Commission, including on behalf of a fund or private fund client. The adviser would have to report by submitting a new Form ADV-C. These confidential reports would bolster the efficiency and effectiveness of the Commission's efforts to protect investors by helping the Commission monitor and evaluate the effects of a cybersecurity incident on an adviser and its clients, as well as assess the potential systemic risks affecting financial markets more broadly.

Disclosure of Cybersecurity Risks and Incidents

Currently, advisers provide disclosures to their prospective and current clients on Form ADV's narrative brochure, or Part 2A, which is publicly available and one of the primary client-facing disclosure documents used by advisers. Form ADV Part 2A contains information about the investment adviser's business practices, fees, risks, conflicts of interest, and disciplinary information. The proposal includes amendments to Form ADV Part 2A to require disclosure of cybersecurity risks and incidents to an adviser's clients and prospective clients.

Like advisers, funds would also be required to provide prospective and current investors with cybersecurity-related disclosures. More specifically, the proposed amendments would require a description of any significant fund cybersecurity incidents that has occurred in the last two fiscal years in funds' registration statements, tagged in a structured data language. The proposal includes

> amendments to Form N-1A, Form N-2, Form N-3, Form N-4, Form N6, Form N-8B-2, and Form S-6.
>
> Recordkeeping
>
> The proposal also includes new recordkeeping requirements under the Advisers Act and Investment Company Act. Rule 204-2, the books and records rule, under the Advisers Act sets forth requirements for maintaining, making, and retaining books and records relating to an adviser's investment advisory business. The proposal would amend this rule to require advisers to maintain certain records related to the proposed cybersecurity risk management rules and the occurrence of cybersecurity incidents. Similarly, proposed rule 38a-2 under the Investment Company Act would require that a fund maintain copies of its cybersecurity policies and procedures and other related records specified under the proposed rule.[45]

IV. COMMENTS ALREADY RECEIVED

We appreciate the many thoughtful comments already received about this important issue. Reproduced below are representative samples from: (1) those advocating for strengthening cybersecurity enforcement; and (2) those suggesting that increased regulation constitutes regulatory overreach.

In Support of Cybersecurity Regulation

In their letter dated February 8, 2022, U.S. Senators Susan M. Collins, Kevin Cramer, Catherine Cortez Masto, Angus S. King, Jr., Jack Reed, Mark R. Warner, and Ron Wyden write to Chairman Gensler as follows:

> Dear Chair Gensler:
>
> We write to urge the Securities and Exchange Commission to propose rules regarding cybersecurity disclosures and reporting. We further urge you to coordinate the formulation of these rules with the National Cyber Director.
>
> As you know, cybersecurity is among our most significant national security and economic challenges. Daily interactions increasingly take place in cyberspace, leading to more persistent and complex cybersecurity threats. Costs of cyber

[45] Fact Sheet, Cybersecurity Risk Management, SEC (March 9. 2023), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sec.gov/files/33-11028-fact-sheet.pdf.

attacks have also been on the rise. Investors often bear these costs because a serious cyber attack can permanently affect a company's valuation and profitability.

During your most recent testimony before the Senate Banking Committee, you stated that you have asked the SEC staff to develop proposals on cybersecurity disclosures and incident reporting. You reiterated in public remarks last month that companies and investors would benefit if information on cybersecurity risk "were presented in a consistent, comparable, and decision-useful manner."

We applaud your efforts to promote transparency and oversight of cybersecurity risks at public companies and at financial sector registrants like investment funds, investment advisers, and broker-dealers. Investors deserve a clear understanding of whether companies and investment managers are prioritizing cybersecurity. They also have a right to prompt notification of serious cybersecurity incidents. More information will enable investors to hold companies and investment managers accountable.

One effective regulatory approach would be asking public companies to disclose whether a cybersecurity expert is on the board of directors, and if not, why not. We have sponsored bipartisan legislation called the Cybersecurity Disclosure Act to require companies to provide this disclosure to investors. The bill does not tell companies how to deal with cybersecurity threats. How a company chooses to address cybersecurity risks would remain its own decision. Boards of directors would be encouraged to develop approaches that address their own needs. The goal is to encourage directors to play a more effective role in cybersecurity risk oversight.

Public companies and investment managers should pay attention to threats before they are realized. This is a better approach than scrambling to figure out what went wrong after investors have been harmed. America's economic prosperity is linked to strong cybersecurity defenses in the private sector. The alternative unfortunately puts investors' hard-earned savings and pensions at risk. We are encouraged that the SEC intends to address cybersecurity threats using a wide variety of tools, from raising the bar on risk management to clarifying when to report a serious breach that has already occurred.

Thank you for your attention to this important matter. Please keep our staffs informed of the SEC's progress on improving cybersecurity disclosures and reporting by public companies and financial sector registrants.[46]

[46] Letter from U.S. Senators Susan M. Collins, Kevin Cramer, Catherine Cortez Masto, Angus S. King, Jr., Jack Reed, Mark R. Warner, and Ron Wyden to Gary Gensler, Chairman, SEC (Feb. 8, 2022), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sec.gov/comments/s7-09-22/s70922-20127532-288660.pdf.

Letters Reflecting Regulatory Overreach Logic

Representative of comments suggesting that this proposed rule is an example of regulatory overreach are those submitted by The Securities Industry and Financial Markets (SIFMA)[47] and SIFMA Asset Management Group ("SIFMA AMG"). The SIFMA provides the following executive summary of their comments:

> Executive Summary
> SIFMA believes the Commission should reconsider its proposals in light of the following:
> • The Commission's proposal of adviser requirements under the antifraud provision of the Investment Advisers Act of 1940 ("Advisers Act") goes beyond that statutory authority. The Commission should instead provide guidance to advisers and funds and coordinate with other federal financial regulators and the Cybersecurity and Infrastructure Security Agency ("CISA") under recently adopted critical infrastructure reporting legislation.
> • If the Commission is committed to creating an additional reporting regime, its proposed 48-hour reporting protocol, involving the onerous completion and submission of Form ADV-C, is unworkable and will not yield useful information for the Commission. The Commission should instead adopt a bifurcated approach: an informal short form notification followed by a more detailed report, without sensitive data, to be submitted after the adviser has had sufficient time to investigate a cyber intrusion.
> • An abbreviated initial notification would align with other regulatory reporting requirements; such harmonization would in turn reduce unnecessary compliance burdens, maximizing an institution's ability to focus on protecting clients and investors during a cyber crisis. Duplicating reporting requirements is not only

[47] Comment on SEC Proposed Rule, File No. S7-04-22 "Cybersecurity Risk Management for Investment Advisors, Registered Investment Companies, and Business Development Companies, SIFMA & SIFMA Asset Mgmt. Group, (April 11, 2022), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sec.gov/comments/s7-04-22/s70422-20123336-279624.pdf.
SIFMA describes itself as:

> the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

inefficient but can damage coordinated cyber incident response at the enterprise level.
• The Commission should provide assurance and documentation of how confidential and high-risk information submitted to the Commission will be protected from intrusion.
• Public disclosure of detailed information relating to cybersecurity incidents or risks is unnecessary and may put members or the financial system at risk.
• The proposed disclosure requirements, particularly the suggested vehicles for disclosure (amended Form ADV Part 2A and the fund prospectus) are onerous, and delivery would require significant burdens and costs. It is too burdensome to require that advisers continually update or revise disclosures and that funds disclose cybersecurity incidents currently affecting it and file prospectus supplements.
• The Commission should adopt a principles-based approach to risk management, as opposed to a "one-size-fits-all" system of policy and control prescriptions.
• To the extent a final rule does include cyber-program requirements or best-practice recommendations, institutions must be able to implement those measures in accordance with an internal assessment; otherwise, the requirements will be too prescriptive.
• Boards should exercise some oversight of cybersecurity programs but should not be compelled to formally approve or review all cyber policies and functions.[48]

V. IN SUPPORT OF CHAIRMAN GENSLER'S CYBERSECURITY INITIATIVE

We wish to lend our support and voice to applaud the leadership by Chairman Gensler in his continued efforts to strengthen responsible cybersecurity among market entity participants. Our thanks also to the staff of the Commission for their hard work on this important initiative. We believe that no issue presents more of a threat to U.S. corporations, securities market participants, and the global economy than those related to cyber attack and data theft. Thank you for the opportunity to comment.

[48] Comment on SEC Proposed Rule, File No. S7-04-22 "Cybersecurity Risk Management for Investment Advisors, Registered Investment Companies, and Business Development Companies, SIFMA & SIFMA Asset Mgmt. Group, (April 11, 2022), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sec.gov/comments/s7-04-22/s70422-20123336-279624.pdf.

Very truly yours,

Neal Newman
Professor of Law
Texas A&M University School of Law
1515 Commerce Street | Fort Worth, TX 76102
Ph: 817.212.4138
- -
www.law.tamu.edu

Lawrence J. Trautman
Associate Professor, Business Law & Ethics
Special Assistant to the Dean for Research and Faculty Development
Prairie View A&M University
Faculty, Texas A&M University School of Law (By Courtesy)
External Affiliate, Indiana University Bloomington, Ostrom Workshops in
Data Management & Information Governance, and Cybersecurity & Internet Governance
SSRN author page: http://ssrn.com/author=1603406