COMMITTEE ON COMPLIANCE

PATRICK T. CAMPBELL
CHAIR
45 ROCKEFELLER PLAZA
NEW YORK, NY 10111
(212) 589-4643
PCampbell@BakerLaw.com

ADAM FELSENTHAL
SECRETARY
165 MASON STREET, 3RD FLOOR
GREENWICH, CT 06830
afelsenthal@gppfunds.com

COMMITTEE ON PRIVATE INVESTMENT FUNDS

MICHAEL S. HONG
CHAIR
450 LEXINGTON AVENUE
NEW YORK, NY 10017
(212) 450-4048
Michael.Hong@DavisPolk.com

MICHAEL W. BRASHER
SECRETARY
450 LEXINGTON AVENUE
NEW YORK, NY 10017
Michael.Brasher@davispolk.com

COMMITTEE ON INVESTMENT MANAGEMENT REGULATION

JOHN FITZGERALD
CHAIR
90 HUDSON ST
JERSEY CITY, NJ 07302
johnfitzgerald728@gmail.com

JUSTIN L. BROWDER
SECRETARY
1875 K STREET, N.W.
WASHINGTON, DC 20006
jbrowder@willkie.com

April 11, 2022

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street N.E.
Washington, D.C. 20549

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Investment Advisers Act Release No. 5956; File No. S7-04-22)

Dear Ms. Countryman:

The Committee on Compliance, the Committee on Private Investment Funds and the Committee on Investment Management Regulation of the New York City Bar Association (collectively, the "**Committees**") respectfully submit this comment letter in response to the Securities and Exchange Commission's (the "**Commission**") proposal to adopt, among other things, Rule 204-6 and Rule 206(4)-9 (the "**Proposal**") under the Investment Advisers Act of 1940 (the "**Advisers Act**").[1] The Committees are composed of lawyers with diverse perspectives on investment management issues, including attorneys from law

[1] The Proposal would also adopt Rule 38a-2 under the Investment Company Act of 1940 (the "**1940 Act**").

firms, counsel and compliance professionals to financial services firms, investment company complexes, investment advisers and investors in private funds.

The Proposal imposes significant new cybersecurity requirements for registered investment advisers and investment funds, including requirements that they maintain written cybersecurity policies "reasonably designed to address cybersecurity risks," that they conduct periodic risk assessments and oversee third-party vendor compliance, that they provide near-immediate notice to the Commission in the event of significant cybersecurity incidents, and that they make certain public disclosures regarding cybersecurity risks and recent experiences (if any) with significant cybersecurity incidents.[2]

The Commission explains that the Proposal was designed to address a number of concerns, including: (a) the increasing frequency and severity of cyber-attacks; (b) the risks to financial markets posed by such attacks; (c) the desire to improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks; and (d) the perceived need for investors to have greater transparency regarding the cyber risks faced by advisers and funds.

While we appreciate the Commission's desire to find ways to address risks related to cybersecurity, which we agree constitute a serious concern for investors and merit investor protections, we believe the Proposal should be modified in several respects.

First, the Proposal's 48-hour notification requirement should be modified on the basis that, in our opinion, it is likely to cause more harm than good. A 48-hour breach notification requirement is nearly unprecedented, and is inconsistent with practically all other notification requirement frameworks in place within the United States. We appreciate the Commission's interest in gaining a greater understanding of security incidents with potential systemic implication, but it is unclear from the proposal why such an aggressive timeline is necessary or appropriate. It is likewise unclear why the Commission's goals could not be met as effectively with a notification requirement that is more consistent with existing regulatory standards and expectations. We remain concerned that, if the Proposal were adopted as proposed, victims of significant security incidents would be forced to divert critical resources toward initial notification and continuous 48-hour updating, which would necessarily decrease the effectiveness of the actual response efforts, and increase the very risks the Proposal is aimed at reducing. At the same time, we believe any significant security incident – one that has implications for sensitive personal or financial information, or that would impact funds' or investment advisers' ability to conduct business and meet contractual obligations – will almost certainly be the subject of other notification requirements under one or more existing regulatory frameworks.

As such, we believe the Proposal should be modified to remove the 48-hour notification requirement, and replace it with a flexible standard that requires notification (a) promptly and no later than 30 days after the determination that a significant cybersecurity incident

[2] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, SEC Release No. IA-5956 (Feb. 9, 2022), 87 FR 13524 (Mar. 9, 2022) (the "**Proposing Release**").

has occurred, or (b) at the same time notification is provided to any other regulator or government entity, whichever is sooner.

Second, we believe the Proposal paints with too broad a brush in applying to nearly all registered investment advisers and nearly all funds managed by those advisers, including private funds that are not registered under the 1940 Act. The stated rationales in support of the Proposal do not appear, on their face, to be based on experience or specific concerns related to all such advisers and funds. As explained below, at a minimum, the Proposal should be modified to exempt funds that rely on the exclusions in Sections 3(c)(1) or 3(c)(7) under the 1940 Act ("**Private Funds**") and investment advisers to Private Funds registered under the Advisers Act ("**Private Fund Advisers**").[3]

Third and finally, the Proposal imposes significant compliance burdens and costs on the entire investment management industry, without taking into account the diversity of funds and investment advisory activities, and with only unclear or speculative benefits. The Proposal's controls-related requirements, including compliance obligations, should be modified to require maintenance of reasonable cybersecurity policies and procedures, the substance of which would be determined by advisers based on a risk-based analysis of their individual circumstances.

While we believe the Proposal is reasonable in ambition, we urge the Commission to consider further whether its ends can be achieved as effectively, more reliably, and at lower cost, with the revisions described below. Absent further evidence-based support for the current proposed requirements, we remain concerned that adoption of the rules as proposed would not advance the Commission's mission to protect investors, maintain fair and orderly markets, and facilitate capital formation.

I. The 48-hour notification requirement in the Proposal is unsupported by evidence and would do more harm than good.

As noted above, a 48-hour breach notification requirement is nearly unprecedented, and would be inconsistent with practically all other notification requirement frameworks that are in place at either the federal or state level. Creating an immediate disclosure regime that is out of step with other disclosure regimes would impose a sizable burden on funds and their advisers. Yet the Proposing Release does not appear to provide "reasons for believing that more good than harm will come of" the 48-hour notification requirement. *Md. People's Counsel v. FERC*, 761 F.2d 768, 779 (D.C. Cir. 1985). We believe a more flexible reporting standard that ensures prompt, but not unreasonably aggressive, notification to the Commission regarding significant cybersecurity incidents would more appropriately balance the competing considerations of (a) the Commission's interest in gaining increased awareness of cybersecurity incidents, and (b) the investment

[3] Alternatively, the Commission should consider exempting from the requirements of the Proposal (in whole, or in part, including the notification requirement) Private Fund Advisers, registered fund advisers, Private Funds, and registered funds whose assets under management or assets fall below a defined, systemic-risk-based threshold.

management industry's collective interest in detecting, containing, responding to, and recovering from cybersecurity incidents that may affect markets and investors.

The Proposing Release explains that the 48-hour notification regime (which includes not only initial notification within 48 hours, but also successive updates within 48 hours of certain changes and events) is intended to help the Commission staff "to understand the nature and extent of a particular cybersecurity incident and the firm's response to the incident" and enable the Commission to "assess the potential systemic risks affecting financial markets more broadly."[4] However, the benefits suggested by the Commission appear largely speculative, and we believe the approach taken by the Proposal should be modified for a number of reasons.

First, the Proposing Release does not offer support for the assumption that a 48-hour requirement will produce the benefits sought by the Commission. We appreciate the Commission's assertion that 48-hour notification would allow the Commission to respond to, and limit, systemic risk. But, as a historical matter, we are aware of no reason to believe that lack of notification to the Commission has contributed to systemic risk. And we find little support for the idea that earlier and more frequent notification to the Commission would have permitted the Commission's staff to take any action that would have prevented investor losses or promoted market stability.

To the contrary, in the context of a serious cybersecurity incident, 48 hours is a vanishingly small amount of time, and frequently insufficient to allow firms to meaningfully assess and understand the nature of an incident they may be experiencing. As a result, the Proposal will likely result in *over* reporting of incidents since scope and significance would be difficult, if not impossible, to determine on that timeline. Such over reporting will have the ancillary effect of making it difficult for the Commission to make use of the data it receives, as it would consist mostly of low-value but high-volume reports.

Second, the aggressive 48-hour notification requirement would distract from the shared goal of detecting, containing, responding to, and recovering from, a security incident. In the midst of responding to a serious business-disrupting event, resources are often in extremely short supply, and the speed of a response is an important factor in determining its success. For this reason, we believe requiring advisers to divert and deploy already limited resources to the task of initial Commission reporting – followed by continuous 48-hour updates for new factual developments (which are virtually certain to arise on a near-daily basis at the start of many incident response efforts) – is not merely unproductive, it is actively harmful.

Third, the Proposing Release does not appear to consider interactions with existing notification requirements, and it does not account for the value in reducing conflicts where possible between notification regimes. Such a broad 48-hour notification requirement is nearly unprecedented at both the federal and state levels, and the need to track and satisfy competing and inconsistent reporting requirements will undermine response efforts, creating enforcement risk and increasing costs for no discernable benefit. The majority of

[4] Proposing Release at 13536.

state breach notification laws – which are, for the vast majority of businesses, the only notification laws that apply to their activities – require notification "as expeditiously as possible and without unreasonable delay."[5] Those that do specify timelines typically offer at least 30 days and as much as 90 days, for notification.[6] Even the New York Department of Financial Services – widely regarded as having an aggressive timeline for incident reporting – provides 72 hours in which to respond. (23 CRR-NY 500.17.) The same is true for the more aggressive industry standards seen in commercial contracts, which usually call for 72 hours or rely on a reasonableness standard. Perhaps the only comparable reporting requirement affording less than 72 hours for notification is under the bank regulatory rules, which require banks to provide notification of a much narrower set of incidents to their primary regulator within 36 hours. (86 Fed. Reg. 66424 (Nov. 23, 2021).) In our view, there is little reason to believe incidents at investment advisers and investments funds would present the kind of systemic risks presented by cybersecurity incidents affecting banking institutions.[7] There does not appear to be any reason therefore why a timeline that is more in line with existing notification obligations would be insufficient to achieve the purposes of the Proposal.

Fourth, and importantly, the 48-hour timeline is inconsistent with the approach taken by Congress in the recently enacted Cyber Incident Reporting For Critical Infrastructure Act of 2022 ("**CIRCIA**"), which imposes a 72-hour timeline for certain covered entities that own and operate federally designated critical infrastructure.[8] There is nothing in the Proposal to justify imposing a more rapid timeline for investment advisers and the funds they advise – and imposing such a requirement would be fundamentally inconsistent with (and possibly preempted by) the legislative treatment of the same issue.[9] We note also that the 72-hour notification requirements under CIRCIA will not apply to all critical infrastructure owners and operators. Congress has tasked the Cybersecurity and Infrastructure Agency ("**CISA**") with designating a subset of covered entities to whom the rules should apply. That is, Congress has expressly acknowledged that – even among the universe of critical infrastructure owners and operators, which include financial service

[5] *See* International Association of Privacy Professionals, State Breach Notification Chart (available online at https://iapp.org/resources/article/state-data-breach-notification-chart/) (last checked Apr. 9, 2022).
[6] *Id.*
[7] Likewise, the Transportation Security Agency has imposed more aggressive breach notification requirements for several categories of owners and operators of critical infrastructure, including "higher-risk" freight railroads, passenger rail, and rail transit owners and operators (*see* Press Release, TSA, DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators (Dec. 2, 2021), https://www.tsa.gov/news/press/releases/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation (24 hours)), critical-designated hazardous liquid and natural gas pipeline owners and operators (*see* TSA, Security Directive Pipeline-2021-01 (May 27, 2021) (12 hours)), and all other pipeline owners and operators (*see* TSA, Information Circular Pipeline-2022-02 (Feb. 16, 2022) (24 hours requested, but not required)). While the clear public health and safety concerns implicated by incidents at such entities may be sufficient to justify near-immediate reporting, those concerns are plainly not presented by incidents occurring at investment funds and investment advisers.
[8] CIRCIA was included as part of the Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, H.R. 2471, 117th Cong., 990-1011 (2022).
[9] Regardless of whether the technical requirements of preemption are met, Congress clearly considered the subject of federal cyber incident reporting requirements in adopting CIRCIA, and the Commission should defer to the legislative policy judgments reflected in that law.

companies – a 72-hour timeline was likely unnecessary and unreasonable for some entities. The Commission should modify the Proposal to defer to that legislative determination.

Fifth, the 48-hour timeline is conceptually at odds with the Commission's own concurrent rulemaking efforts with respect to public companies. On March 9, 2022, the Commission proposed cybersecurity disclosure mandates for public companies, including requirements that public companies disclose material cybersecurity incidents within four business days of determining such an incident has occurred. The Proposing Release does not appear to explain why funds and their advisers should not be afforded the same amount of time to report incidents as public companies, which historically have had greater disclosure requirements.

Sixth, and relatedly, the Proposing Release does not explain why the expected benefits from the 48-hour requirement could not be achieved just as effectively (and at more reasonable cost) by a more flexible reporting requirement or one that aligns with existing vehicles for public-private coordination. For example, through the Financial Services Information Sharing and Analysis Center ("**FS-ISAC**") – a non-profit, member-driven organization created as a result of executive branch action – there is already a robust level of public-private information sharing and coordination overseen by CISA and blessed by Congress. The Proposal does not appear to contemplate the comparative value of this existing framework, or why notification to the Commission in particular would be a better means of reducing systemic risk that could arise as a result of a pervasive security incident. We appreciate that an animating concern behind the Proposal may be a lack of coordination among federal agencies with overlapping responsibility for cybersecurity risks. Respectfully, however, we believe the Proposal is an inappropriate means of addressing that problem insofar as it puts the responsibility for ensuring adequate reporting on industry and on the victims of security incidents, when it should be addressed through better coordination among government agencies.

In sum, any significant incident is already likely to be reported to one or more state, federal, or other sector-specific regulatory bodies. Congress acknowledged the costs and inefficiencies that can result from overlapping, inconsistent reporting regimes in passing CIRCIA. Therefore, we ask that the Commission consider modifying the Proposal to remove the 48-hour notification requirement, and replace it with a more flexible standard that requires notification either (a) promptly and no later than 30 days after determination that a significant cybersecurity incident has occurred, or (b) at the same time as any notification is provided to any other regulator or government entity, whichever occurs sooner.

II. The Proposal should be modified to exempt Private Funds and Private Fund Advisers.

We believe the Proposal would be enhanced if it were modified to exclude Private Funds and Private Fund Advisers. As noted above, the reasoning provided in the Proposing Release expressed in support of the Proposal does not appear tailored to consider the diversity of activities and risks faced by various funds and their advisers, as well as the diversity of fund investors. The Proposing Release appears to assume that the concerns

cited by the Commission in support have materialized equally across the universe of investment advisers and investment funds. Yet there is good reason to believe the rationales offered simply do not apply to Private Funds and Private Fund Advisers.

The Proposing Release cites evidence that cybersecurity risks are, and have been, increasing for some time – a fact that is not subject to serious debate. Respectfully, however, the Commission does not provide support for the idea that these increased risks have uniquely or specifically impacted Private Funds, Private Fund Advisers, or their investors, as such. And we are not aware of any support to suggest that security incidents at Private Funds or Private Fund Advisers present the kind of systemic or individual risks that the Commission cites in support of the Proposal. For example:

- We are aware of no evidence that Private Funds, Private Fund Advisers, or their investors have experienced unique losses, or face any unique risks, related to cybersecurity (and certainly no evidence sufficient to justify the costs and burdens envisioned by the Proposal).

- We are aware of no evidence that Private Fund investors lack confidence due to insufficient information regarding cyber incidents (and the substantial capital committed to Private Funds year over year suggests the opposite is likely true).

- We are aware of no evidence to support the assumption that investors in Private Funds have been harmed due to lack of disclosure, or that they would benefit from additional information regarding cybersecurity incidents experienced by Private Funds and Private Fund Advisers.

- Finally, and as discussed above, we are aware of no evidence that near-immediate notification by Private Fund Advisers of cybersecurity incidents would enable the Commission to take any action that would reduce risks or harms experienced by Private Fund investors or by the market at large.

In addition, the Proposal does not appear to account for the existing understanding and relationship between Private Funds and their investors. Private Fund investors are generally regarded as sophisticated parties who can, and do, obtain the information and protections they require for investing. As a result of investor demands, many Private Funds already have cybersecurity policies and procedures in place as necessary predicates for raising capital. It is commonplace for these policies and procedures to address topics like the implementation of two-factor authentication, as well as other topics and areas of importance to Private Fund investors. We are aware of no evidence that investors who choose to invest in Private Funds without such measures do so unknowingly or without a sufficient understanding of the costs and benefits of their decisions. Likewise, we see no reason to believe that the information required to be disclosed under the Proposal – information that Private Fund investors may not have chosen to request themselves prior to investment – would help Private Fund investors make better investment decisions. At the same time, it is clear that the Proposal would impose significant costs on Private Funds and Private Fund advisers – costs that would, in one respect or another, be absorbed by Private Fund investors. The Proposal therefore would supplant the judgement of Private

Fund investors regarding their own information and diligence needs, at significant cost to those investors, and for only speculative benefits.

The Proposal also risks undermining the investors' choices to commit capital outside the protections otherwise offered in the public markets. Indeed, the Proposal would yield the bizarre outcome that investment funds and advisers are required to provide greater notification and disclosure about their operations, their experience with prior incidents, and their fund clients' prior experiences with security incidents than public companies are required to disclose about the same subjects.[10] This inversion reflects a fundamental change in policy regarding the relationship between public and private markets – a change that is neither justified nor, in our opinion, meaningfully contemplated in the Commission's proposal.

For these reasons, we believe the application of the Proposal to Private Funds and Private Fund Advisers is unsupported, and that the Proposal should be modified – at a minimum – to exempt such funds and advisers or, in the alternative, to provide an asset-size-based threshold under which the requirements would not apply.

III. The cybersecurity policies and procedures requirements of the Proposal are unduly burdensome and unjustified.

The Proposal requires that advisers develop and maintain various categories of cybersecurity policies and procedures, including policies and procedures for conducting risk assessments, for user security and access, for information protection, for cybersecurity threat and vulnerability management, as well as for cybersecurity incident response and recovery.[11] These requirements apply equally to all advisers, without regard to their size, investment strategy, or the unique risks associated with particular funds or adviser activities. But both the costs and benefits (if any) of these controls will vary greatly

[10] On March 9, 2022, the SEC proposed rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, which includes cybersecurity disclosure mandates for public companies. Assuming this proposed rule is passed, it would still not put investment fund advisers and public companies on the same footing, as public companies would be given four business days to provide initial external reporting of *material* security incidents whereas investment advisers would only have 48 hours to report a broader range of *significant* security incidents.
We appreciate that the four-day requirement under the public company rules would require disclosure *to the public* via Form 8-K, whereas the 48-hour notification requirement under the Proposal would require confidential notification *to the Commission* via Form ADV-C. And we do strongly support the confidential treatment of any such Form ADV-C filings as necessary to avoid increased risk to victims during and after a security incident. But if both sets of rules were to be adopted as proposed, *all* public companies would still be afforded more time to externally report a narrower universe of incidents as compared to *all* investment fund advisers. We are aware of no support for such a disparity.

[11] Under the Proposal, advisers and funds would be required to document that the adviser or fund is requiring service providers, pursuant to a written contract, to implement and maintain appropriate measures designed to protect adviser and fund information and systems. We request that, at the very least, the Commission clarify that for funds registered under the 1940 Act, investment advisers and sub-advisers need not obtain fund shareholder approval of such contracts (or amendments to existing advisory contracts to include the relevant provisions) pursuant to Section 15 of the 1940 Act because such agreements (or provisions) are not part of the investment advisory services provided by the adviser and, in any event, would not be material to the fund shareholders.

depending on the fund size and activities, and the Proposing Release does not appear to meaningfully consider that dynamic trade-off.

We appreciate that such an analysis may be difficult to conduct, in all likelihood. But that is due in part to the fact that the substantive policy and procedure requirements under the Proposal are equal parts uncertain and inflexible. The Proposal offers little guidance for industry members and compliance officers trying to understand the precise scope and nature of the policy and procedure requirements to which they may be subject. The Proposal is ambiguous, for instance, as to whether multi-factor authentication is specifically required under Rule 206(4)-9(a)(2), and if so whether the requirement applies equally to all information systems, all employees, and all degrees of access, or whether risk-based determinations can be made based on the facts and circumstances of a particular adviser's business.

Likewise, the requirement under Rule 206(4)-9(b) that advisers conduct periodic (at least annual) risk assessments – and specifically that the assessments include the creation of data inventories covering all fund data and all data provided to third-party service providers – appears absolute, and would be imposed without regard to the reasonable costs and benefits of such activities. But comprehensive data inventories are difficult to conduct and expensive to maintain – a phenomenon that would increase exponentially if the Commission were to approve rules that involuntarily increased demand for such services. Yet the Proposal does not appear to include any economic assessment of the value of such activities, when applied across the spectrum of fund and adviser activities. Nor does it offer clarity as to the granularity and scope required for such activities.

Finally, the requirement under Rule 206(4)-9(a)(3)(ii) that investment advisers exercise "oversight" of third-party vendor security appears ambiguous, unsupported, and arguably unachievable in many instances. It may be reasonable to require certain advisers to include contractual requirements related to information security, and to mandate that those requirements include measures to protect certain sensitive information or systems of the adviser. We do not believe it is reasonable, however, to require that every adviser – without exception, without regard to the number of third-party service providers at issue, and whether or not the adviser even has an information security department of its own – oversee the information security programs of third-party companies simply based on their delivery of vendor services.[12]

The inflexible, yet ambiguous, nature of these and other requirements means that advisers will necessarily be forced to implement compliance controls that are inappropriate for their businesses, that serve no material benefit to investors, that do not contribute to market stability, and that effectively transform otherwise-qualified compliance officers into unqualified information security officers. We are concerned that this will not only result

[12] To this end, it is important to note that many fund advisers rely heavily on third-party information security specialists to provide information technology and security for investment funds. While some advisers are large enough to support large information security teams, most have very limited numbers of employees and rely heavily on outside service providers. Fund advisers should be given the latitude to retain information security specialists to develop cybersecurity policies and procedures that are appropriate for the size and scale of the adviser, and the Proposal should be modified accordingly.

in waste and increased costs, but that it will also necessarily reduce competition among advisers, reduce investor choice, and reduce market efficiency.

Therefore, in addition to providing greater clarity regarding the scope and substance of various requirements, we ask that the Commission consider whether the Proposal's controls-related requirements should be modified to require maintenance of reasonable cybersecurity policies and procedures, the substance of which would be determined by advisers based on a risk-based analysis of their individual circumstances. At the very least, we ask that the Commission modify it to eliminate the three requirements specifically noted above.

We therefore respectfully request that the Commission revise the Proposal as detailed above.

***

The Committees appreciate the opportunity to comment on the Proposal. If we can be of any further assistance in this regard, please contact Patrick Campbell at (212) 589-4643 or Michael Hong at (212) 450-4048.

Respectfully,

Patrick T. Campbell
Chair, Compliance Committee

Michael S. Hong
Chair, Private Investment Funds Committee

John Fitzgerald
Chair, Investment Management Regulation Committee

cc: The Honorable Gary Gensler
The Honorable Caroline Crenshaw
The Honorable Allison Herren Lee
The Honorable Hester Peirce

Drafting Subcommittee:

The Committees would like to express their gratitude to Robert A. Cohen, Matthew A. Kelly, Aaron Gilbride and Matt Bolin of Davis Polk & Wardwell LLP, Michelle Reed, Barbara Niederkofler, Natasha Kohn, and Elazar Guttman of Akin Gump Strauss Hauer & Feld LLP, and Heather McArn, Monique Horton, Jerome Walker, and Andrew Tobel for their assistance in drafting this letter.