DRAWBRIDGE

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

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies. File Number S7-04-22

Dear Secretary:

On behalf of Drawbridge Partners, LLC, please accept this letter in response to the Securities and Exchange Commission's request for comments for the proposed rule "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," File Number S7-04-22.

As a cybersecurity software and services firm with a focus on providing alternative investment firms assistance with their cybersecurity posture, we welcome both the position the SEC has taken and the opportunity to provide our opinion based on the extensive experience we have with SEC-registered Advisers and Funds. We have laid out our comments and matched them to the question numbers within the proposal.

We look forward to the response from the SEC after the comment period has closed and wish to make ourselves available for further review, questions, and engagement from the SEC on this important topic.

Yours faithfully,

Jason Elmer, Chief Executive Officer
Simon Eyre, Chief Information Security Officer

Question 2

Should we scale the proposed requirements based on the size of the adviser or fund? If so, which of the elements described below should not be required for smaller advisers or funds? How would we define such smaller advisers or funds? For example, should we define such advisers and funds based on the thresholds that the Commission uses for purposes of the Regulatory Flexibility Act? Would using different thresholds based on assets under management, such as $150 million or $200 million, be appropriate? Would another threshold be more suitable, such as one based on an adviser's or fund's limited operations, staffing, revenues or management?

The Commission could certainly adjust the expectations based on the size of an adviser or fund's strategy and operations staff. This may be particularly relevant in cases where the strategy does not involve significant liquid assets or revenue, where operations staff and/or processes are meaningfully outsourced, and/or where the number of counterparties overall is limited.

However, there should be time allowed for preparation in advance of reaching a "critical mass" profile. This could be achieved by introducing a "grace period" after reaching this "critical mass," during which an adviser or fund is permitted to bolster any necessary measures before it is subjected to enforcement action.

Question 3

Are the proposed elements of the cybersecurity policies and procedures appropriate? Should we modify or delete any of the proposed elements? Why or why not? For example, should advisers and funds be required, as proposed, to conduct a risk assessment as part of their cybersecurity policies and procedures? Should we require that a risk assessment include specific components (*e.g.,* identification and documentation of vulnerabilities and threats, identification of the business effect of threats and likelihood of incidents occurring, identification and prioritization of responses), or require written documentation for risk assessments? Should the rules require policies and procedures related to user security and access, as well as information protection?

Under section II "DISCUSSION" A, 1, d Threat and Vulnerability Management (page 29), the proposal discusses "threat and vulnerability and response training" with examples for IT Professionals, Developers, Employees, and Executives. Our client experience suggests that this is a key element to any cybersecurity program. While the Commission is avoiding hard rules, we believe that requiring an adequate training program should become a required element of the new rules.

Online and on-demand courses are readily available and affordable to advisors and funds and offer a high level of adaptability. Mandating fundamental awareness training would assist those

few funds or advisers that might not enforce training for all staff (including executives and VIPs). Further or enhanced training for IT and Developer Staff (or other categories, based on the risks identified in the assessments) can be provided as mitigations to the identified risks.

We would also suggest that the risk assessment strategy has been unnecessarily limited to an asset-based risk assessment and a third-party risk assessment. While the discussion within the proposal highlights other identification techniques like threat intelligence, and suggests that remote workers may need different controls, these considerations do not continue to the proposed rules themselves. This may inadvertently lead to the creation of cybersecurity policies and risk management programs that do not address cyber risks associated with known threats, personnel, and events. Regarding personnel, socially engineered attacks, physical security, and logical assets like virtual machines may be excluded under this schema, creating potentially unmitigated pools of risks. We would recommend a clearer rule that allows expansion of risk management techniques.

Question 4

Should there be additional or more specific requirements for who would implement an adviser's or fund's cybersecurity program? For example, should we require an adviser or fund to specify an individual, such as a chief information security officer, or group of individuals as responsible for implementing the program or parts thereof? Why or why not? If so, should such an individual or group of individuals be required to have certain qualifications or experience related to cybersecurity, and if so, what type of qualifications or experience should be required?

We agree with the proposal's discussion points around not enforcing the creation of a CISO, or other particularly certified or qualified person in a cybersecurity-focused role, within all covered organizations. Doing so may cause a significant financial burden on smaller funds. There are a limited number of skilled individuals to fill these roles, and this scarcity would likely put pressure on the cyber industry in other business verticals as well.

Question 5

The Investment Company Act compliance rule prohibits the fund's officers, directors, employees, adviser, principal underwriter, or any person acting under the direction of these persons, from directly or indirectly taking any action to coerce, manipulate, mislead or fraudulently influence the fund's chief compliance officer in the performance of her responsibilities under the rule in order to protect the chief compliance officer from undue influence by those seeking to conceal non-compliance with the Federal

securities laws. Should we adopt a similar prohibition for those administering a fund's or adviser's cybersecurity policies and procedures? Why or why not?

There is a similar requirement within GDPR to implement a Data Protection Officer (DPO) in organizations where large-scale processing of data subjects is in place. We believe that a similar approach may be possible here, in that larger investment funds and advisers could be suitable for such protections. However, that would require "banding" of funds which goes against much of the concept of these rules. We believe enforcing that on a smaller fund/adviser (much like requiring a CISO or particular certified person to implement the cyber program) would be a significant burden.

Question 6

Would advisers and funds expect to use sub-advisers or other third parties to administer their cybersecurity programs? If so, to what extent and in what manner? Should there be additional or specific requirements for advisers and funds that delegate cybersecurity management responsibilities to a sub-adviser or third party? If so, what requirements and why?

We believe the proposal lends itself well to fostering innovation and development within the cybersecurity marketplace. By opening these requirements to include third parties, firms such as expert advisers, consultancies, and technology providers can help develop and implement cybersecurity programs for funds and advisers. We are already part of a growing industry focused on financial services cybersecurity, and we continue to believe our collective knowledge will create significant value for mid-sized and smaller funds that will look to third parties to meet these requirements.

In terms of additional or specific requirements, if an outside provider is performing third-party risk assessments, it should not be possible for them to complete their own risk assessment for presentation to the adviser, fund (and board), as well as the annual SEC report, if they are deemed an important service provider.

Question 7

Should we include any other cybersecurity program administration requirements? If so, what? For example, should we include a requirement for training staff responsible for day-to-day management of the program? If we require such training, should that involve setting minimum qualifications for staff responsible for carrying out the requirements of the program? Why or why not?

While the ownership of a fund or adviser's cybersecurity program is the responsibility of the firm, it may be appropriate for them to outsource the day-to-day tasks normally delivered by a SOC or IT team such as malware detection, user access control, and abnormal behavior monitoring to a third-party MSP or MSSP. It would be cumbersome for a fund to maintain a third party's credentials. The MSP/MSSP/SOC third party should be reviewed as part of the annual third-party risk assessment requirements and the fund or adviser can determine if they are, and continue to be, suitable to provide the services provided to the fund or adviser.

Question 9

What are best practices that commenters have developed or are aware of with respect to the types of measures that must be implemented as part of the proposed cybersecurity risk management rules or, alternatively, are there any measures that commenters have found to be ineffective or relatively less effective?

We note that there is limited discussion within the proposal around penetration testing and nothing solidified in the proposed rules themselves. We agree that penetration testing does not need to become a compulsory element of the rule set.

In our experience, Vulnerability Management provides the foundation for a secure environment and should be the standard prerequisite to penetration testing in most use cases. Penetration testing is a point-in-time exercise, whereas Vulnerability Management will provide the firm with continuous oversight. This kind of continuous Vulnerability Management provides an ongoing, real-time (or near real-time) service to the fund or adviser, helping to keep secure their services, updates, and technology in a way that point-in-time penetration testing cannot provide. The costs are also generally lower for Vulnerability Management services versus penetration testing, and the costs to perform penetration testing can vary greatly depending on the scope of the test (e.g., external, internal, black/grey/white box testing, and socially engineered penetration testing).

Funds and advisers may yet identify penetration testing to be a suitable risk control, particularly for those involved with in-house software development or with a large presence on the Internet. Therefore, penetration testing can remain a control choice for the fund or adviser, though not one that we feel must necessarily be made compulsory for all firms.

Question 10

What user measures do advisers currently have for using mobile devices or other ways to access adviser or fund information systems remotely? Should we require advisers and funds to implement specific measures to secure remote access technologies?

> With the move to hybrid and remote working conditions affecting many technology implementations, it is important to ensure the cybersecurity controls in place within a traditional work environment can meet the needs these new styles of working conditions present. Computers (in particular, laptops) have joined the traditional "mobile" management schemes. With the technology that funds and advisers use changing rapidly (for example, Mobile Device Management is being largely overtaken by Mobile Application Management in BYOD office environments), it would be difficult to stipulate a specific requirement. Rather, the goal should be to ensure a flexible regulatory framework that encourages funds and advisers to take all necessary and reasonable measures to secure their data, regardless of the network or device that touches it.

Question 12

Other than what is required to be reported under proposed rule 204-6, should we require any specific measures within an adviser's policies and procedures with respect to cybersecurity incident response and recovery?

> The Commission may consider using this opportunity to call out Cyber Insurance as a potential protective measure. While it may not be suitable for all, there should at the very least be an evaluation (in the annual assessment) of the benefits of having a policy available which may cover the costs of recovery, and also provide access to resources to assist with such efforts.

Question 13

Should we require that advisers and funds respond to cybersecurity incidents within a specific timeframe? If so, what would be an appropriate timeframe?

> Once an event or series of events has been identified as a cybersecurity incident, it is broadly recommended and expected that incident response actions be initiated without any timeframe or delay. Those first moments are often the most critical in minimizing impact. As such, any guidance or regulation concerning the timeframe within which to activate incident response procedures should be based upon the moment of discovery of a potential breach.

Question 14

Should we require advisers and funds to assess the compliance of all service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access adviser or fund information systems and any adviser or fund information residing therein, with these proposed cybersecurity risk management rules? Should we expand or narrow this set of service providers? For example, with respect to funds, should this requirement only apply to "named service providers" as discussed above?

> We agree with the proposal that service providers should not be limited to just "named service providers." The selection process should be based on the processing of data and those third parties that may represent additional risk to the business.
>
> For example, this may include IT Managed Service Providers and SaaS trading platforms like Order Management Systems and Execution Management Systems. It would be good to clarify if the personal data of staff at a fund or adviser is also considered as covered within the rules and as such, whether other third parties (such as outsourced HR) may be considered in scope.

Question 18

Do advisers or funds currently consider their or their service providers' insurance policies, if any, when responding to cybersecurity incidents? Why or why not?

> (Please also refer to our response to question 12 concerning Cyber Insurance.) We would agree that this should be evaluated across service providers as well, particularly those where a significant disruption in operation and/or breach of data would significantly affect the fund or adviser's operation.

Question 19

Are advisers and funds currently able to obtain information from or about their service providers' cybersecurity practices (*e.g.,* policies, procedures, and controls) to effectively assess them? What, if any, challenges do advisers and funds currently have in obtaining such information? Are certain advisers or funds (*e.g.*, smaller or larger firms) more easily able to obtain such information?

> Managers are obtaining this information through the vendor due diligence (VDD) process. Due to the varying nature of funds' and advisers' third parties, and of VDD processes themselves, responses are often inconsistent or not applicable. Some larger third parties (e.g., "Big 4" accounting firms, bulge bracket banks), typically refer to publicly available information which does not provide evidence of a strong cybersecurity posture or potential gaps in their programs.

This results in less clarity for funds and advisers as to whether or not there are requirements for vendors to provide timeline notifications of breaches, similar to what is proposed in this bill. Having the ability to obtain standardized forms like SOC Reports and ISO Certifications would assist with obtaining relevant and consistent information.

Question 21

Is the proposed requirement for advisers and funds to review their cybersecurity policies and procedures at least annually appropriate? Is this minimum review period too long or too short? Why or why not?

Annual reviews are a suitable cadence as long as funds are running a real-time risk management process (e.g., continuous vulnerability management, continuous vendor due diligence, and continuous risk checks). It would allow sufficient evidence to be gathered to analyze the impact of changes to the cyber policies and procedures without being too reactionary to individual events (for example, some technical cybersecurity controls may take several weeks or even months to properly configure and align to the business thresholds and behavior).

There could be a reasonable requirement to also perform a review of policies on a substantial change to the business or technology. For example, changing a fund administrator or IT MSP (or indeed, changing from in-house to outsourcing, or vice versa) could also be reason for interim review.

Question 22

Should the annual review include whether the cybersecurity policies and procedures reflect changes in cybersecurity risk over the time period covered by the review? Why or why not?

Cyber risk is continually changing based on new and evolving threats. The security controls must adapt to those changing conditions and that can only happen with a recurring review of risk. Examples of conditions which may trigger a change in a fund or adviser's risk profile might include growing to critical mass around AUM and/or headcount, changes in regions where staff may reside and/or travel to, investment or operational strategy shifts, significant changes to and/or increases in counterparties, etc.

In general, it should be the goal both of written policies and of regulation covering funds and advisers to develop processes and controls which are flexible enough to account for a constantly evolving risk landscape.

Question 25

Are there any conflicts of interest if the same adviser or fund officers implement the cybersecurity program and also conduct the annual review? How can those conflicts be mitigated or eliminated? Should advisers and funds be required to have their cybersecurity policies and procedures periodically audited by an independent third party to assess their design and effectiveness? Why or why not? If so, are there particular cybersecurity-focused audits or assessments that should be required, and should any such audits or assessments be required to be performed by particular professionals (*e.g.,* certified public accountants)? Would there be any challenges in obtaining such audits, particularly for smaller advisers or funds?

> Much of the compilation of information for the proposed cybersecurity program and the subsequent annual review will likely require multiple business divisions, as well as assistance from a third-party cybersecurity vendor, service provider, or specialist. We envision that this collaboration will help funds and advisers police themselves. However, one aspect around the risk assessments may require special attention.
>
> The risk assessments will likely require the primary IT team (whether internal IT or a third party such as an MSP) to provide evidence and complete the assessment itself, which may be a conflict of interest of "marking their own homework." Similarly, if a cybersecurity firm is brought in to provide their services to assist with the fund or adviser's cybersecurity program, it may also be suggested that they need to provide an independent assessment (if the data they hold about the fund or adviser is considered critical and/or sensitive).

Question 26

Should the Commission require a fund's board, including a majority of its independent directors, initially to approve the cybersecurity policies and procedures, as proposed? As an alternative, should the Commission require approval by the board, but not specify that this approval also must include approval by a majority of the fund's directors who are not interested persons of the fund? Why or why not?

> It would make sense not only for board members to initially approve cybersecurity policies and procedures, but also to be part of the annual review process. This will help to ensure that the review is conducted in accordance with the requirements outlined, and also because many board members may have relevant experience and/or viewpoints which would be additive to the creation and upkeep of the firm's cybersecurity policies and procedures.

Question 27

As part of their oversight function, should fund boards also be required to approve the cybersecurity policies and procedures of certain of the fund's service providers (*e.g.*, its investment adviser, principal underwriter, administrator, and transfer agent)? Why or why not? If so, which service providers should be included and why?

> If a third-party risk assessment includes the requirement to ensure the service provider meets or exceeds the information security policies and procedures of the fund or adviser, it is likely this requirement will be redundant.

Question 33

Are the records that we propose to require advisers and funds to keep relating to the proposed cybersecurity risk management rules appropriate? Why or why not? Should advisers and funds have to keep any additional or fewer records, and if so, what records?

> We see these measures as appropriate, particularly to show the evolution of a program as a firm changes its operation as described above. The amount of documentation should be minimal and should be easy to maintain locally.

Question 34

Do advisers or funds have concerns it will be difficult to retain any of documents? Could this place an undue burden on smaller advisers or funds?

> The amount of documentation should be minimal and should be easy to maintain locally.

Question 37

Who should be responsible for having a reasonable basis to conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident or that one is occurring? Should the Commission require a person or role be designated to be the one responsible for gathering relevant information about the incident and having a reasonable basis to conclude that such an incident occurred?

> There can often be significant confusion and misunderstanding during an incident. It would make sense for each fund or adviser to have a responsible party with the appropriate skill set to be prepared to act as the designee for such declarations. If there is no employee with this skill

set, the firm should seek out advice from an appropriate third party – MSP, MSSP, Legal, Compliance, etc. – who can advise.

Question 38

At what point would one conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident? Would it be after some reasonable period of assessment or some other point?

It may make sense for an adviser to outline these thresholds in advance, perhaps in their Written Information Security Policy (WISP). For example, if an adviser is unable to manage a portfolio for a predetermined and agreed-upon time frame (which could be as little as minutes or as long as a full day, depending on the portfolio and strategy), and/or if it is determined that data which has been predetermined to be sensitive in some way has been breached, it would be deemed a significant event.

Question 41

Do commenters believe requiring the report 48 hours after having a reasonable basis to conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident or that one is occurring is appropriate? If not, is it too long or too short? Should we require a specific time frame at all? Do commenters believe that "a reasonable basis" is a clear standard? If not, what other standard should we use?

For consistency with other rulings including the "Cyber Incident Reporting for Critical Infrastructure Act" (CIRA), it may be worth considering the same 72-hour period for reporting.

Question 42

Should we provide for one or more exceptions to the reporting of significant cybersecurity incidents, for example for smaller advisers or funds? Are there ways, other than the filing of Form ADV-C, we should require advisers to notify the Commission regarding significant cybersecurity incidents?

The concern with requiring submission of an ADV-C filing and the associated public reporting is that the details of the incident would be vague and open to interpretation, especially soon after it is discovered. This may potentially put the adviser at a disadvantage which could be unwarranted. The situation could be compared to a CarFax report, which only states that an accident occurred without providing any real detail, yet it still devalues the car tremendously – even if the accident turns out to be a minor one.

Question 48

Will the proposed cybersecurity disclosures in Item 20 of Form ADV Part 2A be helpful for clients and investors? Are there additional cybersecurity disclosures we should consider adding to Item 20? Should we modify or delete any of the proposed cybersecurity disclosures?

> The proposed disclosures in principle should not represent a risk to advisers as long as required disclosures concerning "how they assess, prioritize, and address cybersecurity risks" (pg. 170, Proposed Amendments to Form ADV Part 2A) remain at a high level. Any element requiring disclosure of the controls in place puts useful information into the hands of a threat actor and should be minimized.

Question 58

Should the rule include a requirement to disclose whether a significant fund cybersecurity incident is currently affecting the fund as proposed? Why or why not? How often should cybersecurity disclosure be updated? Is the lookback period of two fiscal years appropriate? Why or why not?

> Record keeping for a historical two-year period may prove to be difficult for a fund if they are required to backdate the disclosure prior to the rule being enforced. Situations such as changing an MSP might result in a lack of available details as requested in the Form. As such, there should be reasonable concessions that incidents prior to the ruling may lack all requested details. We may take lessons from the implementation of MiFID II in Europe. The regulation was passed with an enforcement date set some years in the future, allowing covered firms to design and implement new policies and procedures in time for the enforcement date.