

April 11, 2022

Ms. Vanessa Countryman
Secretary, Office of the Secretary
US Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

RE: Comments on SEC Release Nos. 33-11028; 34-94197; IA-5956; IC-34497; File No. S7-04-22 RIN 3235-AN08 Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

Ms. Countryman:

On March 9, 2022, the US Securities and Exchange Commission (SEC or Commission) proposed new rules under the Investment Advisers Act of 1940 (“Advisers Act”) and the Investment Company Act of 1940 (“Investment Company Act”) to require registered investment advisers (“advisers”) and investment companies (“funds”) to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks; to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients to the Commission; to make certain disclosures related to significant cybersecurity risks and cybersecurity incidents that affect advisers and funds and their clients and shareholders; and to comply with new recordkeeping requirements under the Advisers Act and Investment Company Act.

NRS, a ComplySci Company, appreciates the opportunity to comment on this important proposal and respectfully submits the following response. Cybersecurity risks are a clear, present, and growing threat to advisers and funds, and the investors they serve. In our experience, the vast majority of the firms covered by this rule are actively addressing these risks, consistent with their fiduciary duty to their customers. NRS commends the SEC for proposing this rule which, if adopted, will establish minimum standards that will be consistently implemented across the industry.

Background on NRS and NRS Clients

Since 1983, NRS has provided its clients with exceptional compliance consulting services, compliance technology solutions, education conferences and seminars. In addition, NRS created and sponsors, in conjunction with the Investment Adviser Association, the Investment Adviser Certified Compliance Professional (IACCP®) certification program, which has produced more than 1,000 designees. NRS serves more than 3,000 investment advisers, broker-dealers, and investment companies ranging from small firms to the largest global investment management complexes and myriad firms in between.

Over our 39 years of providing consulting services, NRS has continually interacted with investment advisers of all sizes through our conferences, seminars, and consulting relationships. We have learned that regulatory clarity and precision is a strong determinant of effective compliance. Investment advisers, broker-dealers and other financial institutions must clearly understand the expectations of regulators and their obligations under applicable regulations in order to design and implement effective compliance controls that ultimately serve to protect investors.

It has also been our experience that many small and mid-sized advisers believe that they are disproportionately affected by the cost of complying with new regulations, many of which address risks far more common among firms much larger than they. Particularly in the evolving landscape of cybersecurity, advisers with limited staff and resources must be able to allocate their resources to the highest and best use and should not be forced into a Faustian bargain which prioritizes regulatory reporting over the critical and time-sensitive work required to effectively mitigate an active threat. NRS agrees that regulatory reporting and client disclosures should be thorough and timely; for firms with fewer resources, we believe a risk-based approach would be more consistent with the current risk-based protocols that are a hallmark of investment adviser compliance programs and more conducive to the attainment of the industry's collective goal of protecting investors.

We urge the Commission to consider adopting thresholds for compliance with certain proposed changes and to weigh the benefits of increasing regulatory reporting requirements (including the amount of time advisers are given following a key event to make required filings) against the time and expense required to properly research, analyze, prepare and file those reports and to address and mitigate the effect of cyber incidents on clients and investors.

NRS appreciates the opportunity to comment on the Commission's proposed amendments; our responses to specific questions included in the Release follow.

Section II. A. Cybersecurity Risk Management Policies and Procedures

Question 1. *Should we exempt certain types of advisers or funds from these proposed cybersecurity risk management rules? If so, which ones, and why? For example, is there a subset of funds or advisers with operations so limited or staffs so small that the adoption of cybersecurity risk management programs is not beneficial?*

NRS Response: NRS' experience with advisers of all sizes and providing all types of services leads us to conclude that all advisers would benefit from cybersecurity risk programs. That said, the nature and scope of the rules for each firm should be based on the risks posed by each firm's business practices. In our opinion, any adviser or fund, regardless of size or business practices, that holds PII data, insider information or other sensitive information should adopt a cybersecurity risk management program tailored to their specific risks. NRS suggests that the Commission adopt an approach that assigns advisers to various risk-based categories (or tiers). For example, one initial set of categories could be:

- Lower risk – Advisers that do not possess identifying information about individual investors. An example of this would be a pension consultant that, while providing advice to many plans and their participants, does not retain identifying information about plan participants.
- Medium risk – Advisers that do possess identifying information about individual investors but do not permit access to their systems by third parties (excepting third-party firms providing information technology consulting and management services [hereinafter “managed service providers”]). An example is an advisory firm that uses trading platforms supplied by a custodian broker that is entirely separate from the adviser's own information systems.
- Higher risk – Advisers whose own systems and data can be accessed by third parties. An example is an adviser that permits third parties access to its own trading or portfolio management systems to provide reports and updates to the adviser's system.

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?*

NRS Response: Within the framework described in our response to Question #1, NRS agrees that staffing, revenues, nature of services provided, and other factors may be considered in determining the extent to which various provisions of the proposed rule would apply. NRS suggests that, rather than establishing bright-line thresholds for applying these additional thresholds, the Commission require that advisers consider these factors when assessing risks and developing appropriate policies and procedures, and that the firm’s conclusions regarding the applicability of these factors to that firm’s business be documented in a written risk assessment.

Section II. A. 1. e. Cybersecurity Incident Response and Recovery

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?*

NRS Response: In the years since Investment Advisers Act rule 206(4)-7 (the “Compliance Program Rule”) was adopted, it has proven to be a practical and effective framework for firms of all sizes to prevent, detect and correct violations of the securities laws. This risk-based approach can be equally effective in developing cybersecurity programs. The elements of the cybersecurity policies and procedures should parallel those of the Compliance Program Rule by:

- Requiring a written risk assessment, written policies and procedures, and a written annual review; and
- Providing guidance (rather than rules) for content in the adopting release and subsequent communications (such as risk alerts, FAQs, etc.)
- Require a designated CISO (see Question #4 below)

Given the scope and specialized nature of cybersecurity programs, and to avoid duplication of effort, NRS recommends that risk assessments, policies and procedures, and annual reviews prepared under this rule be considered sufficient to address cybersecurity risk under the Compliance Program Rule.

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?*

NRS Response: NRS again recommends that the Commission follow the successful model of the Compliance Program Rule by requiring that an individual be named as Chief Information Security Officer (“CISO”) and that such individual must have the knowledge, competence, and authority to discharge their duties. NRS does not recommend any formal requirements beyond that, although, we further recommend that the Commission clearly establishes the liability carried by a person assuming the CISO role.

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?*

NRS Response: The highly complex and rapidly-evolving nature of threats to information systems requires specialized knowledge and insight. To ensure that small and mid-sized advisers can have access to this knowledge, the Commission should permit firms to outsource the CISO function.

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?*

NRS Response: As risks continue to evolve, staff responsible for day-to-day program management must be alert to current and emerging risks. The rule should require training for these staff members, but should allow each adviser to determine the nature and content of that training based on its own risk profile.

NRS recommends that the Commission avoid being too prescriptive in its rulemaking to allow for the market to develop solutions that are innovative, effective and efficient. For example, vendor managed Virtual Desktop solutions exist today (including from an affiliate of NRS, Itegria) that are specifically designed for Investment Advisers, that take regulatory requirements into consideration as a foundation

for their technology needs, and are a good mechanism to allow even small and medium sized firms to address many information security needs from a single third party. These types of solutions simplify the administration of cyber security programs by utilizing the resources and expertise of the third-party provider.

Question 8. *Are the proposed rules' definitions appropriate and clear? If not, how could these definitions be clarified within the context of the proposed rules? Should any be modified or eliminated? Are any of them proposed terms too broad or too narrow? Are there other terms that we should define?*

NRS Response: The vast majority of advisers understand the rationale behind regulatory requirements and make earnest efforts to comply. When faced with a situation requiring an urgent response, advisers need concrete, unambiguous guidance. If advisers are left to their own devices to interpret the Commission's intent, the same fact pattern faced by multiple advisers will lead to myriad responses; this would appear to be adverse to the industry's interests and the Commission's intent in proposing such requirements. NRS recommends that the Commission provide examples and fact patterns to illustrate scenarios contemplated by the Commission when selecting the definitions used.

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?*

NRS Response: No. In working to develop effective and practical policies and procedures for advisers with a small number of employees, or for advisers in the lower risk category discussed in our response to Question #1, NRS has found that these firms will respond to virtually all incidents by contacting (a) their Managed Service Providers to identify, mitigate, and correct the problem and assess any loss of data, (b) their attorneys to identify their duties to clients and regulators, and (c) their insurance providers to determine if any losses are covered. This response does not change based on the nature of the incident. NRS does recommend that incident response and recovery procedures be required, but that these procedures be developed by each firm based on the nature of their own business practices.

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?*

NRS Response: NRS is concerned that requiring a specific timeframe may distract advisers from focusing on identifying, mitigating, and correcting the effects of a cybersecurity incident. Furthermore, during a severe incident, the fund or adviser may be working closely with law enforcement authorities who may deem disclosure a hindrance to their efforts. Therefore, NRS believes a requirement to report incidents “promptly” is sufficient.

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?*

NRS Response: It has for some time been an acknowledged best practice for advisers to conduct due diligence on third-party service providers. In keeping with the risk-based nature of adviser regulation, NRS believes that advisers are in the best position to evaluate their relationships with service providers and determine what type of due diligence and oversight is appropriate. Mandating these requirements for advisers could penalize smaller firms lacking the resources or influence to compel third-party service providers to comply with requests for such information and would seem to be of little value when advisers have no client information and/or do not allow third-party access to client information.

Question 17. *Should we require advisers' and funds' cybersecurity policies and procedures to require oversight of certain service providers, including that such service providers implement and maintain appropriate measures designed to protect a fund's or an adviser's information and information systems pursuant to written contract? Do advisers and funds currently include specific cybersecurity and data protection provisions in their agreements with service providers? If so, what provisions are the most important? Do they address potential cybersecurity risks that could result from a cybersecurity incident occurring at a fourth party? Should any contractual provisions be specifically required as part of these rules? Should this requirement apply to a more limited subset of service providers? If so, which service providers? For example, should we require funds to include such provisions in their agreements with advisers that would be subject to proposed rule 206(4)-9? Are there other ways we should require protective actions by service providers?*

NRS Response: The most effective way to address the very real concerns posed by the possibility of third- or fourth-party cybersecurity incidents is for each adviser to evaluate its own relationships with third parties and conduct the due diligence and oversight it deems appropriate based on the identified risks. Requiring a one-size-fits-all approach for all advisers would likely result in policies and procedures

that are more aspirational than practical. Although in many cases market forces have already compelled the inclusion of contractual cybersecurity provisions which accrue to the benefit of all advisers, it is possible that some firms without sufficient resources or influence may not be able to compel or enforce such contractual provisions, which would then likely result in a violation of policies and procedures. Mandating these requirements for all advisers may also cause insurmountable burdens on third-party service providers, particularly smaller or specialized firms, which could result in the inability of advisers to access much-needed services. Firms with sufficient resources and influence are more likely to be those with many relationships with third-party service providers and the concomitant risks, consistent with the high-risk category discussed in our response to Question #1; NRS believes the imposition of requirements based on the assessment of risks is both practical and effective.

Section II. A. 2. Annual Review and Required Written Reports

***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?*

NRS Response: NRS does not believe there are any inherent conflicts in having the same adviser or fund officers responsible for implementing and testing the cybersecurity program – no different than AML or insider trading. Smaller firms are likely to be adversely and disproportionately impacted by an independent third-party assessment requirement. Any requirement that specifies minimum qualifications of third parties permitted to conduct such reviews could have unintended consequences by creating a large and sudden demand among what may be an insufficient number of qualified third parties. The value of independent third-party assessment is immeasurable, as many advisers have learned by voluntarily engaging independent third-party assistance to comply with the annual review requirements under 206(4)-7. Similarly, NRS believes the determination as to whether to engage third-party assistance to evaluate its cybersecurity policies and procedures is best left to the adviser based on their risk assessment and staff capabilities.

Section II. B. 1. Proposed Rule 204-6

Question 43. *The Commission recently proposed current reporting requirements that would require large hedge fund advisers to file a current report on Form PF within one business day of the occurrence of a reporting event at a qualifying hedge fund that they advise.⁶⁹ The proposed reporting events include a significant disruption or degradation of the reporting fund's key operations, which could include a significant cybersecurity incident. If the amendments to Form PF are adopted, should the Commission provide an exception to the Form ADV-C filing requirements when an adviser has reported the incident as a current report on Form PF? Alternatively, should the Commission provide an exception to the Form PF current reporting requirements if the adviser filed a Form ADV-C in connection with the reporting event?*

NRS Response: Multiple filings regarding the same cybersecurity incident, required within such a short time period following an incident, could result in the diversion of a firm's resources that would be better spent on the time-critical tasks of investigating, mitigating and communicating in the immediate aftermath of a cybersecurity incident. While the benefit of such reporting is clear, the diversion of resources during such a sensitive time could prevent the firm from focusing on minimizing harm to clients and investors. Streamlining reporting requirements would make it easier for advisers to comply, while saving valuable time that could be utilized for other critical tasks.

Section II. B. 2. Form ADV-C

Question 45. *Is IARD the appropriate system for investment advisers to file Form ADV-C with the Commission? Instead of expanding the IARD system to receive Form ADV-C filings, should the Commission utilize some other system, such as the Electronic Data Gathering, Analysis, and Retrieval System (EDGAR)? If so, please explain. What would be the comparative advantages and disadvantages and costs and benefits of utilizing a system other than IARD? What other issues, if any, should the Commission consider in connection with electronic filing?*

NRS Response: Many advisers enlist the support of third-party service providers when required to make EDGAR filings due to the perceived difficulty of use. When faced with an unanticipated need to file quickly, the third-party service providers on which such firms often rely may be unavailable. Most advisers are already familiar with the IARD system and would find it easier to navigate than EDGAR. When a new filing is required, particularly within a short timeframe, the advantages of allowing use of the system most familiar to the majority of advisers are clear.

Question 47. *Should Form ADV-C be confidential, as proposed? Alternatively, should we require public disclosure of some or all of the information included in Form ADV-C?*

NRS Response: Form ADV-C should be confidential, as proposed. Advisers are already subject to public disclosure requirements that would likely require reporting of the most serious cybersecurity incidents. Mandating a publicly available filing could have a chilling effect on advisers, who may err on the side of non-disclosure if there is any ambiguity or uncertainty as to whether filing is required. A confidential filing would be most likely to result in the proactive and timely reporting of information which is fundamental to the Commission's goals of early detection of emerging threats with possible market-wide impact.

Section II. C. 3. Requirement to Deliver Certain Interim Brochure Amendments to Existing Clients

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?*

NRS Response: Advisers are already compelled to disclose information that would reasonably be considered an important factor in an investor's evaluation of whether to work with or continue to work with an adviser. A serious cybersecurity incident could conceivably require disclosure under existing rules; as such, an additional section in ADV 2A may not convey any additional benefit. Because many investors may not be able to distinguish between the most serious cybersecurity incidents and the increasingly frequent incidents of a less serious nature, advisers erring on the side of caution by disclosing more information will not compare favorably with advisers who determine that the circumstances of their cybersecurity incident did not warrant disclosure. The desire to avoid public and client disclosure, and the potential competitive disadvantage for those that do, could create a chilling effect preventing future disclosures.

Question 49. *Does the definition of significant adviser cybersecurity incident allow advisers to inform investors of cybersecurity risks arising from the incident while protecting the adviser and its clients from threat actors who might use that information for the current or future attacks? Does this definition allow for disclosures relevant to investors without providing so much information as to be desensitizing? Why or why not?*

NRS Response: It is likely that detailed disclosures could desensitize investors, thus reducing the impact of cybersecurity incident disclosures and all disclosures generally. Depending upon the details provided and relevant circumstances, it is possible that such disclosures may work to the advantage of threat

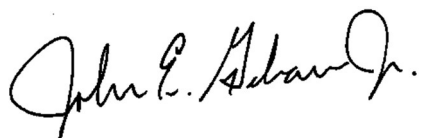
actors at the expense of investors and the adviser. Any ambiguity or uncertainty as to what incidents would rise to the level of investor disclosure or what type or level of detail is required to be disclosed or, conversely, should not be disclosed due to the risk of misuse, could result in additional and unnecessary risk to investors and advisers.

Question 51. *We propose to require advisers to update their cybersecurity disclosures in Item 20 promptly to the extent the disclosures become materially inaccurate. Do commenters agree that the lack of disclosure regarding certain cybersecurity risks and cybersecurity incidents would render an adviser's brochure materially inaccurate? Should we only require advisers to update their cybersecurity disclosures on an annual basis (rather than an ongoing basis, as proposed)?*

NRS Response: In the event that a firm is affected by several cybersecurity incidents and/or defines related cybersecurity incidents as individual incidents rather than one incident, it is conceivable that an adviser's brochure could be perpetually materially inaccurate. If the most serious cybersecurity incidents could be clearly defined, requiring prompt disclosure of those incidents is reasonable. The disclosure of any but the most serious cybersecurity incidents may actually trivialize important disclosures by desensitizing investors, and updates should only be required annually, if required at all.

Thank you for the opportunity to comment on this proposal. We appreciate your consideration of our comments and would be happy to provide any additional information that may help in your endeavor to address this extremely important topic.

Respectfully,

A handwritten signature in black ink, appearing to read "John E. Gebauer". The signature is fluid and cursive, with a large initial "J" and "G".

John Gebauer

President
NRS, a ComplySci Company