Date: December 23, 2022

To: Secretary, U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090
Email: mailto:rule-comments@sec.gov: File Number S7-25-22

From: Andrew Moyad, CEO, Shared Assessments LLC
[redacted]

RE: U.S. SECURITIES AND EXCHANGE COMMISSION 17 CFR Parts 275 and 279:
Proposed Rule § 275.206(4)-11 [Release Nos. IA-6176; File No. S7-25-22]
RIN 3235-AN18—Outsourcing by Investment Advisers

The Shared Assessments Program appreciates the opportunity to submit comments to the U.S. Securities and Exchange Commission.

Shared Assessments has been setting the standard in third party risk assessments since 2005. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body that defines best practices, develops tools, and conducts pace setting research. Shared Assessments Program members work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy, and business resiliency control assessments. Additional information on Shared Assessments is available by visiting: http://www.sharedassessments.org.

On behalf of the Shared Assessments Program and its members, thank you for accepting the following response in regard to the proposed Outsourcing by Investment Advisers Rule, File No. S7-25-22.

Securities & Exchange Commission 17 CFR Parts 275 and 279: Proposed Rule § 275.206(4)-11
[Release Nos. IA-6176; File No. S7-25-22] RIN 3235-AN18—*Outsourcing by Investment Advisers*

Thank you for the opportunity to respond to the SEC's Draft Rule on Outsourcing by Investment Advisers. While the proposed rule covers a complex and evolving landscape that we believe can benefit from selective incremental regulation and management, there are both high level policy and practical operational issues created by the Rule as currently written. While some increase in oversight is warranted and feasible, regulations must be practical, principle-based, risk-based, and appropriately fit viable operating models. We respectfully submit that this draft as written is too tactical and, in some instances, may cause unintended harm to the very interests it is designed to protect, as noted in the below.

Our responses address each of the major areas covered by the Rule and the related Request for Comment Questions.

1) **Scope of the Rule**—*Response*: Elements of the proposed rule are internally and externally inconsistent and duplicative to existing regulations. The Scope of the Rule should be simplified and clarified. Focusing outsourcing regulations around specific elements of robust due diligence and reporting should yield more effective, feasible, and realistic governance practices. An amendment to the existing Compliance Program Rule § 275.206(4)-7 Compliance procedures and practices would provide a practical avenue to implementing more focused and explicit due diligence and monitoring obligations for outsourced services, as those services reasonably fall under the firm's existing fiduciary obligations under Compliance Program Rule 206(4)-7.

   Rationale:
   a) As drafted, the proposed language can be reasonably read so broadly that it could: (1) overly complicate compliance with existing regulations; and (2) be duplicative to much of the due diligence and reporting Investment Advisers already perform as part of their fiduciary and other risk management and monitoring practices. Effective risk management practices are already accepted globally and are incorporated into existing SEC and other domestic and international regulatory requirements for due diligence, inventory management, and compliance.
   b) The incremental value of the Rule as written does not provide sufficient added value for consumers and industry resilience, and creates unintended consequences. For example, the Rule notes that providing information about governance and concentration risk to the public might influence their decision to choose a specific adviser (page 75 of proposed Rule). However, the exposure of the data required to inform consumer choice around concentration risk also provides the opportunity for criminal exploitation of that information and may not provide any clear benefit in a way that meaningfully improves consumer choice. *[Questions: 24, 25, 46]*
   c) Proposed Rule § 275.206(4)-11 in its current form makes it problematic for firms to track and manage the resulting information, and for the SEC to track and manage as the use and the stewardship of sensitive and confidential information obtained is unclear in the Rule. It would be more effective for the SEC to directly address the issues it finds in exams—as noted in the Rule discussions—as an amendment under the existing Compliance Program Rule 206(4)-7. *[Questions: 1, 18, 19, 21, 22, 23, 24, 25, 26, 28, 34, 35, 41, 44, 68, 73, 74, 84, 86, 100]*

2) **ADV Form Proposed Changes**—*Response*: The form should be significantly shortened from its proposed format. While the data made publicly available through the proposed ADV would provide the SEC with deeper insight into potential concentration risk, the stewardship process and how this data will be utilized by the agency to reduce concentration risk are unclear and seem to pose unintended and significant risks (as noted above). The data derived from the ADV would pose a significant compliance and cyber/data risk without meaningful benefit: (a) due to the exposure of the relationships within the sourcing chain, making the chain vulnerable to hacking and other disruption; and (b) would effectively constitute a breach of the expected contractual and potentially ethical wall that Investment Advisers are required to maintain, due to the confidentiality of certain provider relationships. (Many outsourcing agreements forbid either party from disclosing even the existence of the business relationship, let alone other commercial or legal provisions.)

   Rationale:
   The requirement for inventories/registers of service providers is appropriate and is consistent with existing regulations worldwide, and any regulations that the SEC adopts should generally mirror existing regulatory language (e.g., Luxembourg, Germany, EBA, Singapore, OCC). In addition, the SEC draft Rule requirements around divulging business data may conflict with the principles of the European Union's GDPR and California's CCPA. If ADV reports are to be made public, the SEC will have to supervise and deidentify these reports to remain in compliance with (or at least honor the expectations around) these types of data protection rules, as well as protect the original data in-house at the SEC. As a model of effective practice, the manner in which ransomware incidents reported through centralized information hubs are managed by a government agency to provide alerts and advisory on threats can provide examples of how sensitive information is being effectively collected, anonymized, and distributed in a protected manner. *[Questions: 7, 8, 20, 28, 29, 30, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 82, 101]*

3) **Definition of Outsourced Functions**—*Response*: Despite the SEC's stated objective, as written the Rule provides conflicting guidance about the extent to which an Adviser can use risk ranked evaluation of individual outsourced services and providers to set its due diligence standards. The broad nature of the language in the proposed Rule results in a lack of definition around covered functions and does not adequately draw distinction between functions that require regulatory oversight and key functions that allow for service delivery consistent with resilience planning (e.g., administrative functions, CRM, transfer functions, etc.). We recommend the SEC utilize Investment Adviser firm-level risk-ranked, material provider inventory as the basis for compliance and examination. We further recommend that Investment Advisers be required to assess providers during the selection and onboarding processes and through ongoing due diligence, including by application of appropriate contract clauses, addendums, system security, data access, sub sourcing consent assurances as may be feasible for N^{th} parties, and use of other proportional due diligence requirements. There are emerging internationally recognized reasonability standards being developed by other financial regulators—both domestic and international—which could serve as useful frameworks for continued development of SEC N^{th} party guidance. The draft language requires firms to obtain N^{th} party verifications, an issue that regulators globally are just beginning to grapple with. We recommend that the SEC can assist in developing a rational approach to this issue by adopting a more narrow, well-defined view of a smaller number of critical vendors would be more consistent with OCC, PRA, and other emerging regulations.

Rationale:

a) We recommend a determination of materiality that utilizes generally accepted risk management principles and domains. For example, from a data management viewpoint, a 'least privilege data/network access' bill would be more agreeable in determining data access and therefore which providers pose material risks.

b) Providers/services in different risk tiers do not pose the same risks to the firm, its customers, or the market as a whole. In spite of language noting that this Rule is not a one size fits all approach (as noted in Section I.B. page 17, II.3.B. page 42, and II.3.B.2 page 45 and 47) for evaluating potential risks of a specific outsourcing arrangement, the Rule contains seemingly contradictory, prescriptive language around recordkeeping and documentation requirements that are out of scale with whether or not providers are material for that firm (as noted starting on Section II.C.1 beginning on page 69, and II.E starting on page 79 of the proposed Rule). This contradiction can be too easily read as dictating a broad stroke due diligence approach to all providers encouraging firms to respond to interpreting the Rule in the broadest manner to reduce the risk of negative examination findings.

c) The proposed Rule seems to indicate [Section B., page 40] that the SEC will evaluate the appropriateness of a firm's decision to outsource a function. Firms should not be restricted from outsourcing functions they deem reasonable and responsible under their formal outsourcing policies through considerations that include, but are not limited to, the complexity of the function(s), associated risks arising from outsourcing the function(s), and the potential operational impact on the ability to provider critical services in the event of a service disruption. *[Questions: 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 18, 19, 20, 23, 24, 25, 26, 34, 35, 38, 44, 57, 61, 67, 73, 74, 84, 86, (includes 'core' function designation)]*

4) **Due Diligence Requirements**—*Response:* As drafted the Rule would have significant impact on advisory firms of all sizes due to the need for exponential increases in due diligence and reporting personnel and functions to meet the broad and unclear nature of the Rule. We respectfully disagree with the SEC's contention that costs would increase initially and then taper back down once processes and platforms had been established. The Rule is more likely to cause significant staffing cost increases over an extended period. Though initial implementation costs may decline, the costs to any given firm would be increased throughout the life of the Rule due to the overbroad nature of the language that would require firms to increase staffing to respond to interpreting the Rule in the broadest manner to reduce the risk of negative examination findings.

Rationale:

a) The impact on firms includes largely duplicative due diligence that advisers are already required to perform as part of their existing risk management processes, including those around outsourced functions. Even larger firms express that the level of tracking and reporting would cause both immediate and long-term, unsustainable increase in staffing exerting negative and time consuming impacts that would ripple across the firm's departments and providers and ripple-effect costs to clients. *[Questions: (impact/costs) 56, 57, 58, 66, 67, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 84, 87, 88, 89, 90, 91, 92, 93, 95, 96, 97, 98, 99, 100]*

b) Continuous monitoring is increasingly critical and has become widely accepted in today's complex and dynamic environment. Existing language does not acknowledge the important role that continuous monitoring can play in *select* circumstances. We recommend that SEC staff consider the appropriateness of adding continuous monitoring language for critical vendors with a specific focus on testing the effectiveness of critical third (and Nth) party continuous

monitoring programs, as well the effectiveness of continuous monitoring programs sector-wide. *[Questions: includes discussions on contracts, materiality, impact, oversight, and monitoring 2, 17, 27, 28, 29, 31, 32, 33, 34, 36, 37, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49; (monitoring) 50, 51, 52, 53, 54, 55, 70, 71, 94]*

5) **Transition Period for Effective Date of Rule**—*Response*: A 10-month period does not provide adequately for the proposed Rule. The timeline for implementation of the Rule should be consistent with an accurately calculated scope of effort that will be required to comply with the regulation. A transition period of at least 12 months is probably more appropriate, potentially even 18 to 24 months.

   Rationale:
   The Rule as written does not provide firms with the basis for realistic estimates of scope of effort. It is notable that an iterative approach to implementation has been successful for other regulators in this sector; for example, the EU's *Digital Operational Resilience Act (DORA)*. *[Questions: 83, 84, 85]*