Tuesday, December 27, 2022

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

Re: *Outsourcing by Investment Advisers*
File Number S7-25-22
17 CFR Parts 275, and 279
[Release Nos. IA–6176; File No. S7–25–22]
RIN 3235–AN1

Submitted electronically via rule-comments@sec.gov

Dear Secretary Countryman;

Amazon Web Services (AWS)[1] appreciates the opportunity to respond to the Securities and Exchange Commission's (SEC) proposed rule, *Outsourcing by Investment Advisers*, as published in the *Federal Register* on October 26, 2022.[2] As a cloud service provider, AWS welcomes an on-going dialogue with the SEC to bring a technology perspective to the discussion of the due diligence and risk management lifecycle. AWS recognizes the important role of private sector engagement in SEC rulemaking and would welcome a deeper discussion of the responses included in this submission.

In 2006, AWS began offering information technology infrastructure—now commonly known as cloud computing.[3] Today, AWS provides financial firms the secure resilient global cloud infrastructure and services needed to innovate, enhance customer experience, differentiate for growth, and adapt to the needs of tomorrow.[4] AWS now has more than 200 services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence, security, and application development, deployment, and management.[5]

[1] AWS revenue was $18.44 billion in Q1 2022, which grew by 37% year-over-year. AWS annualized revenue run rate was $74 billion in Q1 2022.

[2] 87 Fed. Reg. 68816 (Oct. 29, 2022) (to be codified at 17 C. F. R. 275, 17 C. F. R. 279).

[3] Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, customers can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider. Federal Financial Institutions Examination Council (FFIEC), Joint Statement Security in a Cloud Computing Environment (April 2020) *citing* NIST SP 800-145, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, defines cloud computing as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or third-party service provider interaction."

[4] AWS case studies of global financial services companies can be found here.

[5] Please review the full list of services at the AWS website.

As proposed, the rule would ask advisers to "reasonably determine that it is appropriate to continue to outsource those services or functions to that service provider"[6] by, among other possible options, "periodic onsite visits where other services may be monitored remotely. Methods of monitoring could include, for example, automated scans or reviews of service provider data feeds, periodic meetings with the provider to review service metrics, or contractual obligations to test and approve new systems prior to implementation."[7]

Although the proposed rule does not create new direct obligations for third-party service providers, the use of cloud-based recordkeeping services is a point of emphasis mentioned multiple times in the text.[8] Viewed through the perspective of the Cloud-related Shared Responsibility Model,[9] AWS acknowledges and agrees that the role of risk management within the third-party service provider/customer relationship is important.[10] To avoid burdensome and duplicative efforts, AWS supports a risk-based approach to due diligence and third-party risk management, and reliance on independent certifications, attestations, and industry standards, which have proven effective for nearly two decades. [11]

> Integrating independent certifications, attestations, and industry standards reduces duplicative and burdensome third-party due diligence requirements.
>
> Third-party attestations and certifications provide visibility and independent validation of the control environment. When validated by a qualified, independent third party as part of a risk management and due diligence program, attestations and certifications help address requirements to perform validation work on an IT environment hosted in the cloud. They also can help assure the design and operating effectiveness of control objectives and controls.
>
> AWS supports security standards and compliance certifications to help customers satisfy compliance and risk management requirements globally. AWS achieves third-party validation for thousands of compliance requirements that are continually monitored to help meet security and compliance standards for industries including finance, retail, healthcare, government.[12]

---

[6] Outsourcing by Registered Advisers, 87 Fed. Reg. at 68816.

[7] *Id.*

[8] For example, the rule would "proh bit registered investment advisers from outsourcing certain services or functions without first meeting minimum requirements." Under the proposal, these advisers are "to conduct due diligence prior to engaging a service…and to periodically monitor the performance and reassess the retention of the service provider…." Advisers would be obligated to "reasonably determine that it is appropriate to continue to outsource those services or functions to that service provider." 87 Fed. Reg. 68,816 (Oct. 29, 2022) (to be codified at 17 C. F. R. 275, 17 C. F. R. 279).

[9] The Shared Responsibility Model refers to sharing the responsibility for security and compliance between AWS and the customer. "AWS operates, manages and controls components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. This differentiation of respons bility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud." https://aws.amazon.com/compliance/shared-responsibility-model/

[10] AWS comment letter responding *to Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants*, 86 FR 68300 (proposed Dec. 1, 2021) (to be codified at 17 C.F.R. pt. 240)(Jan. 3, 2022). https://www.sec.gov/comments/s7-19-21/s71921-20111119-264770.pdf *citing* Securities Industry and Financial Markets Association (SIFMA) comment letter (Dec. 22, 2021). https://www.sifma.org/wp-content/uploads/2021/12/SIFMA-Comment-Letter-RE-Electronic-Record-Keeping-Requirements-for-Broker-Dealers-1.pdf

[11] AWS White Paper, *Amazon Web Services: Risk and Compliance* (March 11, 2021). https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/welcome.html

[12] See a list of *AWS Services in Scope by Compliance Program* at: https://aws.amazon.com/compliance/services-in-scope/.

This is accomplished through AWS' participation in over 50 different audit programs and regular independent third-party attestation audits to provide assurance that our control activities are operating as intended.

AWS supports certification, attestation, and industry standards programs, including:

1. National Institute of Standards and Technology (NIST) 800-53, Security and Privacy Controls for Information Systems and Organizations,[13]
2. Payment Card Industry Data Security Standard (PCI-DSS),[14]
3. Federal Risk and Authorization Management Program (FedRAMP),[15]
4. European Union's General Data Protection Regulation (GDPR),[16]
5. Federal Information Processing Standard Publication (FIPS 140-2),[17]
6. International Organization for Standardization (ISO),[18] and
7. Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR).[19]

The AWS audit results are documented by the assessing body and made available for all AWS customers at no cost through an on-demand self-service portal. This allows customers to continuously monitor AWS security and compliance and have access to new audit reports.[20] Customers also benefit from relying on the same security controls AWS uses to secure its own infrastructure. These controls strengthen the compliance and certification programs, while also providing access to tools to reduce costs and ease compliance with industry-specific security assurance requirements.

---

[13] SP 800-53 Rev. 5 (Sept 2020). "This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks." https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[14] The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard and Visa. https://aws.amazon.com/compliance/pci-dss-level-1-faqs/; PCI DSS applies to entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD), including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. https://pcisecuritystandards.org/document_library/. AWS Compliance Guide: *Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 on AWS* (Oct 2020). https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf

[15] FedRAMP is a US government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud products and services. https://www.fedramp.gov/program-basics/ Cloud service providers who want to offer their cloud service offerings to the US government must demonstrate FedRAMP compliance. https://aws.amazon.com/compliance/fedramp/ FedRAMP uses the NIST Special Publication 800 series and requires cloud service providers to complete an independent security assessment conducted by a third-party assessment organization to ensure that authorizations are compliant with the Federal Information Security Management Act (FISMA). https://www.cisa.gov/federal-information-security-modernization-act

[16] GDPR protects European Union individuals' fundamental right to privacy and the protection of personal data. It includes robust requirements that raise and harmonize standards for data protection, security, and compliance. https://aws.amazon.com/compliance/gdpr-center/

[17] The Federal Information Processing Standard (FIPS) Publication 140-2 is a US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information. https://aws.amazon.com/compliance/fips/

[18] ISO/IEC 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidance. https://aws.amazon.com/compliance/iso-27001-faqs/

[19] CSA is a not-for-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing." https://aws.amazon.com/compliance/csa/

[20] AWS Artifact is the central resource for customers to obtain compliance-related information. It provides on-demand access to security and compliance reports from AWS and independent software vendors on AWS Marketplace. https://aws.amazon.com/artifact/

AWS appreciates the SEC's sustained interest in inviting feedback on questions at the crossroads of cloud technology and financial services. On behalf of AWS, I would welcome the opportunity to discuss approaches to due diligence and risk management for registered investment advisers. I am available to coordinate within AWS to support the SEC's work and understanding of cloud services within financial services.

Respectfully,

Denyette DePierro
US Financial Services Lead
AWS Public Policy
[redacted]