Monday, June 5, 2023

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Submitted electronically at rule-comments@sec.gov

Re: File No. S7-05-23; *Regulation S-P: Privacy of Consumer Financial information and Safeguarding Customer Information*; Release Nos. 34-97141; IA-6262; IC-34854 (Regulation S-P)

File No. S7-06-23; *Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents*; Release No. 34-97142 (Rule 10)

File No. S7-04-22; *Reopening of Comment Period for Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*; Release Nos. 33-11167; 34-97144; IA-6263; IC-348555 (Cybersecurity Risk Management)

Dear Ms. Countryman:

Amazon Web Services (AWS) appreciates the opportunity to provide comments to the Securities and Exchange Commission (Commission) on the Regulation S-P, Rule 10, and the Cybersecurity Risk Management proposals.[1] As a cloud service provider, AWS invites an ongoing dialogue with the Commission to bring a third-party technology service provider perspective to the discussion of cybersecurity risk management and incident reporting, and would welcome a deeper discussion of the responses included in this submission.

[1] AWS will submit a separate comment letter on the Commission's pending proposal on Regulation Systems Compliance and Integrity. *Regulation Systems Compliance and Integrity*; 88 Fed. Reg. 23146 (proposed Apr. 14, 2023) (to be codified at 17 C.F.R. pts. 242, 249).

(continued...)

In 2006, AWS began offering information technology infrastructure—now commonly known as cloud computing.[2] Today, AWS provides reliable, secure, scalable, agile, and low-cost cloud infrastructure built to satisfy the most stringent security requirements. AWS operates globally to power businesses of all sizes, ranging from startups to large enterprises and public sector entities. Cybersecurity and operational resilience are essential components of the AWS approach to providing cloud services. Cloud infrastructure enables rapid, cost-effective innovation while enhancing customer security and resilience.[3] AWS consistently implements processes to protect customer data, and enhance the security and resilience of cloud computing and the information technology cybersecurity infrastructure.

AWS supports the Commission's policy goal of "protect[ing] the U.S. securities markets and investors in these markets from the threat resulting from cybersecurity risk."[4] In addition to financial services, the AWS regulated customer operates across a range of industries, including healthcare, education, government, transportation, telecommunications, and energy, among others.[5] As a third-party service provider to the financial services sector, AWS supports customers in asset management, banking, capital markets, insurance, and payments, among other areas.[6]

---

[2] Cloud computing is the on-demand delivery of information technology 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), 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." Fed. Fin. Insts. Examination Council, *Joint Statement Security in a Cloud Computing Environment*, OFFICE OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-46a.pdf (citing Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology* (Special Publ'n 800-145, Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf).

[3] US Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services*, 21 (Feb 2023). "From the perspective of the financial institutions interviewed for this report, the security capabilities for public cloud services generally match or exceed their on-premises capabilities." https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

[4] Rule 10 proposal at 21.

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

[6] AWS case studies of global financial services customers can be found at https://aws.amazon.com/solutions/case-studies/?customer-references-cards.sort-by=item.additionalFields.sortDate&customer-references-cards.sort-order=desc&awsf.content-type=*all&awsf.customer-references-location=*all&awsf.customer-references-

(continued...)

AWS provides financial firms secure, resilient global cloud infrastructure and services to innovate, enhance customer experience, differentiate for growth, and adapt to future technology needs. As an AWS customer, these firms have access to over two-hundred AWS services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence, security, and application development, deployment, and management.[7]

I. AWS encourages close collaboration with other federal agency efforts to ensure a coordinated national approach to cybersecurity.

AWS is committed to working with the Commission and other federal agencies in support of a harmonized approach to cybersecurity that is robust, resilient, and sufficiently flexible to foster continued innovation and technological development, including within the financial services sector. Given the global importance of financial services and technology, coordination among the public and private sectors is essential to building a secure and level playing field for all market participants.[8] Harmonization supports the larger goal of fostering a defragmented, consistent, and fair regulatory framework as the foundation of a thriving innovative financial sector.[9]

---

segment=*all&awsf.customer-references-industry=industry%23financial-services&awsf.customer-references-use-case=*all&awsf.customer-references-tech-category=*all&awsf.customer-references-product=*all.

[7] A full list of AWS's services can be found on the AWS website at https://aws.amazon.com/products/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc&awsf.re%3AInvent=*all&awsf.Free%20Tier%20Type=*all&awsf.tech-category=*all.

[8] The term *market participant*, as used in this comment letter, refers to securities market participants falling within the Commission's remit and regulatory authority. These include broker-dealers, clearing agencies (clearing corporations and depositories), depositories, credit rating agencies, Alternative Trading Systems (ATS), investment advisers, securities exchanges, self-regulatory organizations (SROs), and transfer agents. https://www.investor.gov/introduction-investing/investing-basics/how-stock-markets-work/market-participants For more technical information on Market Participants, visit http://www.sec.gov/divisions/marketreg/mrclearing.shtml.

[9] AWS is not alone in recognizing the importance of harmonizing cybersecurity regulations. In fact, such harmonization was listed as an explicit priority in the recently released U.S. National Cybersecurity Strategy. The Strategy makes clear that "[w]here Federal regulations are in conflict, duplicative, or overly burdensome, regulators must work together to minimize these harms." THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 9 (Mar. 1, 2023) https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. It further states that, "[w]here feasible, regulators should work to harmonize not only regulations and rules but also assessments and audits of regulated entities." *Id.*

(continued...)

The proposed cybersecurity risk management and incident response rules are part of a larger, multi-agency policy trend focusing on the security and resilience of the financial services sector. Recent regulatory proposals, administrative actions, and legislative initiatives, include the 2021 Computer-Security Incident Notification Rule,[10] the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),[11] pending incident response and cybersecurity risk management rules from the Commodity Futures Trading Commission (CFTC)[12] and the New York State Department of Financial Services' Cybersecurity Regulation,[13] and anticipated global recommendations from the Financial Stability Board on Third Party Risk Management in the third quarter of 2023.[14] Each of these efforts overlap in intent and scope with the Commission's proposals. Any additional rulemaking should evaluate existing law and standards, consider the quickly evolving regulatory landscape, and contemplate how the Commission's approach will align with cybersecurity and incident reporting requirements or proposals emerging from other agencies or entities.

II. AWS encourages reliance on established, widely adopted cybersecurity standards, frameworks, and guidelines.

There are several cybersecurity standards, frameworks, and guidelines that are widely adopted and globally respected. These standards, frameworks, and guidelines are able to respond nimbly to evolving threats and technological change. Often developed in close collaboration with private sector experts, the standard setting bodies and entities host robust working groups and quickly integrate public comments and necessary revisions.

---

[10] *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 Fed. Reg. 66424 (proposed Nov. 23, 2021) (to be codified at 12 C.F.R. pts. 53, 225, 304).
[11] Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, 136 STAT. 49, 1038-59 (2022).
[12] *Reporting and Information Requirements for Derivatives Clearing Organizations,* 87 Fed. Reg. 76698 (proposed Dec. 15, 2022) (to be codified at 17 C.F.R. pts. 39, 140).
[13] "The proposed Second Amendment to DFS Cybersecurity Regulation, 23 NYCRR Part 500, was published in the New York State Register on November 9, 2022. Comments were due on January 9, 2023, and we are in the process of reviewing them." (June 3, 2023, 9:52 AM), https://www.dfs.ny.gov/industry_guidance/cybersecurity. 23 NYCRR § 500 (2022).
[14] FIN. STABILITY BD., FSB WORK PROGRAMME FOR 2023, at 5 (2023), https://www.fsb.org/wp-content/uploads/P300323.pdf. The "Indicative timeline of key FSB publications planned for 2023" subsection indicates that the consultative document, *Strengthening financial institutions' ability to manage third-party risks and outsourcing*, is scheduled for publication in July 2023.
(continued...)

These standards, frameworks, and guidelines include the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[15] the NIST Control Objectives for Information and Related Technologies,[16] the International Organization for Standardization (ISO) standards,[17] the Center for Internet Security (CIS) Critical Security Controls,[18] the and Cybersecurity and Infrastructure Security Agency's (CISA) anticipated Cybersecurity Performance Goals (CPG)[19] for the financial services sector, as well as the Cyber Risk Institute's Cybersecurity and Cloud Profiles,[20] which are mapped to global financial services regulations, including the Commission's Regulation Systems Compliance and Integrity (RegSCI). A unified posture for robust, sector-wide cybersecurity would integrate the work of these leading cybersecurity organizations with Commission expectations to shape leading practices. Relying on well-known and widely accepted standards, frameworks, and guidance to inform regulations could address the dual goals of protecting investors with leading cybersecurity practices while offering market participants of all sizes, a substantive, risk-based, least-cost approach to operational resilience and cybersecurity.

III. AWS encourages a pragmatic approach to cybersecurity risk management that considers appropriate timelines, triggers, disclosures, contracting, and technology-informed compliance expectations.

Complementing the suggested focus on harmonization, alignment, and coordination, AWS encourages the Commission to consider a pragmatic approach that supports the shared goal of a resilient financial services sector. The capacity of financial firms and third-party service providers to respond to incidents would be optimized by regulations that enhance security, reinforce operational resilience and are technology informed.

---

[15] NIST, *Cybersecurity Framework*, (last visited June 3, 2023) https://www.nist.gov/cyberframework.
[16] NIST, Security and Privacy Controls for Information Systems and Organizations (Joint Task Force, Special Publication 800-53 Revision 5).
[17] INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/home.html (last visited June 3, 2023).
[18] CTR. FOR INTERNET SEC., CRITICAL SECURITY CONTROLS VERSION 8 (May 2021).
[19] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, CROSS-SECTOR CYBERSECURITY PERFORMANCE GOALS, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (last visited June 3, 2023).
[20] CYBER RISK INST., THE PROFILE, https://cyberriskinstitute.org/the-profile/ (last visited June 3, 2023).

1. Extending timelines for initial incident reporting would allow more complete and accurate disclosures, and minimize the risk of adverse impacts on market participants and investors from responding to active incidents on short timelines.

   Every moment is crucial during a cyber incident response. Significant resources are dedicated to understanding the scope of a potentially critical incident while simultaneously investigating origins, securing systems. and mitigating impacts. During the phase of active investigation and response, the understanding of the facts surrounding an incident may be uncertain as new aspects are uncovered, resolved, or proven unfounded. Early in an investigation, it may be clear that a compromise has occurred, but it may be unclear if systems or data have been impacted. Providing information before an incident has been assessed may lead to confusion and misunderstanding. Initial reports may be subject to continuous revision during an ongoing investigation. Despite the underlying intent of the proposals, frequent disclosures may not lead to clarity. Rather they may lead to confusion and analytical noise as investors learn to ignore voluminous, ever-changing reports.

   As a third-party service provider, AWS also is impacted by regulatory reporting regimes and timelines. AWS may provide incident-relevant information to customers as part of AWS' reporting obligations, subject to internal customer support procedures or as required under AWS customer contracts. AWS urges the Commission to review other incident reporting frameworks' direct and indirect obligations and explore opportunities to coordinate requirements under harmonized rules.

   For instance, the Rule 10 and the Cybersecurity Risk Management proposals establish 48-hour timeframes for initial confidential reporting using prescribed forms and content. These timelines are short—particularly when compared to other reporting regimes. For example, CIRCIA contemplates a 72-hour reporting timeframe for national critical infrastructure, including the financial services sector.[21] Acknowledging the necessity of directing all available resources to addressing, managing, mitigating, and remediating an active incident, AWS encourages the Commission to consider a longer reporting time line to support the dedication of resources needed to discover and mitigate potential harm caused by an incident.

[21] Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, §2242, 136 STAT. 49, 1043 (2022).

2. Clarifying triggers for reporting and amending previously submitted information would ensure resources remain focused on responding to an active incident.

   Complying with notice triggers is an essential and challenging part of the incident response process. Such compliance often requires continuous monitoring of developing facts and ongoing assessment of contractual language and supervisory expectations. AWS urges the Commission to consider clear triggers for reporting obligations and to harmonize triggers among the Commission's regulations and other federal regulatory regimes. AWS also encourages the Commission to consider the practical burden of implementing multiple conflicting reporting triggers and timelines while in the midst of responding to an active incident.

   Relatedly, the Rule 10 and the Cybersecurity Risk Management proposals require prompt (and, in any event, no later than 48 hours) amendments to Form SCIR and Form ADV-C, respectively. Amendments are required when (i) information previously reported becomes materially inaccurate, or (ii) there is new material information to report concerning the incident. The proposed structure of periodic reporting increases the risk of errors and omissions, particularly during the early stages of an incident when information is developing rapidly and materiality may be difficult to assess. Compliance without clear substantive triggers may divert significant resources from incident response and could result in limited incremental information of value, instead contributing to confusion.

3. Eliminating overly prescriptive requirements for incident reporting would allow context-specific and meaningful disclosure, while limiting publication of potentially compromising security information.

   Information from a developing cyber incident can change frequently as the understanding of an incident evolves, which could lead to misinformation and confusion, particularly if the information is shared publicly. Misinformation can negatively impact a public company and any associated third-party service provider. In addition, even the disclosure of accurate information causes concern as the disclosure of detailed information about cyber incidents can prompt further incidents, as threat actors access public reporting to discover new technical vulnerabilities and identify potential targets.

Accordingly, public disclosure requirements should be thoughtfully crafted, carefully timed, and balance the value of full transparency with the potential harms to individual firms and the sector as a whole.

The Rule 10 and the Cybersecurity Risk Management proposals require periodic public disclosure of significant cyber events, including whether they are active and ongoing. AWS encourages the Commission to consider whether modifying these requirements may be appropriate to avoid further risk to the reporting entity and the financial services sector.

4. Accommodating existing private party contracts and relationships with third-party service providers would reduce the risk of regulatory fragmentation and conflicting obligations.

The proposals call for specified contractual arrangements with third-party service providers.[22] As regulatory regimes develop, there is increased risk of fragmented regulatory frameworks, and of mandatory contract regimes containing overlapping, duplicative, and contradictory obligations. Conflicting obligations will delay implementation, yield inefficient results, and reduce transparency for investors.

Adopting the contractual portions of the proposals will require consideration of the burden placed on a financial sector that operates under several competing regulatory regimes. AWS provides cloud services to several customers participating in multiple industries subject to differing regulations administered by different agencies, each with differing requirements. Within the financial services sector, AWS supports several financial firms that are regulated by more than one supervisor and regulatory regime.

---

[22] *See, e.g.*, Cybersecurity Risk Management proposal at 87 (noting that "the proposal requires registrants to include contractual provisions in its agreements with service providers to guarantee adherence to required measures"); Regulation S-P proposal at 34 ("Specifically, these policies and procedures would require covered institutions, pursuant to a written contract between the covered institution and its service providers, to require service providers to take appropriate measures that are designed to protect against unauthorized access to our use of customer information."); Rule 10 proposal at 108 ("Further, pursuant to that written contract, the service provider would be required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of proposed Rule 10, that are designed to protect the Covered Entity's information systems and information residing on those systems.").

Given this regulatory complexity, AWS suggests that the Commission defer to private parties to draft contractual provisions. Financial firms of the size, sophistication, and complexity to be subject to multiple regulatory regimes have the expertise to negotiate mutually agreeable arrangements with third-party service providers. Taking this approach allows the Commission to remain faithful to its regulatory goals without inadvertently creating implementation friction by requiring parties to negotiate contractual provisions that may be inapplicable or have unintended negative effects.

If the rules, when implemented, include contractual requirements, it will be crucial to grant an extended phase-in period for contract review and revision.[23] AWS suggests a minimum of two years. This phase-in will facilitate negotiating and adding compliant language to existing agreements. Prematurely reopening the private, commercial contractual relationships between customers and third-party service providers is overly burdensome and should be avoided.

5. Fostering flexibility in compliance may bring more efficient, practical, situationally reasonable, and technology informed risk management solutions.

   Third-party service providers are challenged to react to new regulations across geographies, customer-types, industries, services, sectors, and regulatory regimes. The Commission's consideration of the practical difficulty of implementing aspects of the proposals is appreciated. AWS acknowledges and agrees that the role of risk management within the third-party service provider relationship is important.[24]

---

[23] In addition to the immediate proposals, the SEC's other recent rulemakings, such as 17a-4, 18a-6, and the anticipated RegSCI, also are introducing due diligence reviews and contractual revisions. These concurrent obligations on contractual language would burden the same firms and the same employees with duplicative obligations to review and repaper potentially thousands of customer and third-party service provider relationships across industry at the same time. This compliance churn will burden resources and limit the availability to meet regulatory deadlines.

[24] The importance of risk management in the third-party service provider relationship is reflected in the Shared Responsibility Model (SRM). This 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

(continued...)

Flexibility in compliance and risk management may offer answers to implementation challenges that are more efficient, practical, and situationally reasonable.

Cyber risk assessments and third-party information gathering could integrate reliance on independent certifications, attestations, and industry standards.

To avoid burdensome and duplicative efforts, AWS supports a risk-based approach to due diligence and third-party risk management that integrates reliance on independent certifications, attestations, and industry standards, which have proven effective for nearly two decades.[25] 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 ensure the design and operating effectiveness of control objectives and controls.

AWS urges the Commission to consider approaches allowing third-party service providers to offer customers standardized, but objectively complete information. Rule 10 would require Covered Entities to prepare annual written reports[26] assessing the cyber risk of information systems, potentially requiring significant additional information from third-party service providers.

---

responsibility is commonly referred to as security "of" the cloud versus security "in" the cloud." AMAZON WEB SERVICES, SHARED RESPONSIBILITY MODEL, https://aws.amazon.com/compliance/shared-responsibility-model/
This has been acknowledged in prior AWS comment letters. *See, e.g.*, Amazon Web Services, Comment Letter on Proposed Rule for Electronic Recordkeeping Requirements, https://www.sec.gov/comments/s7-19-21/s71921-20111119-264770.pdf (citing Securities Industry and Financial Markets Association (SIFMA), Comment Letter on Proposed Rule for Electronic Recordkeeping Requirements (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.

[25] *See* Amazon Web Services, White Paper, Amazon Web Services: *Risk and Compliance* (Mar. 11, 2021), https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-risk-and-compliance/aws-risk-and-compliance.pdf#welcome.

[26] Rule 10 proposal at 96.

(continued...)

AWS supports security standards and compliance certifications to help customers satisfy compliance and risk management requirements globally. At AWS, this is achieved through 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, and government. AWS participates 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 a variety of certifications, attestations, and industry standards programs, including NIST 800-53,[27] *Security and Privacy Controls for Information Systems and Organizations*, the Payment Card Industry Data Security Standard (PCI-DSS),[28] the Federal Risk and Authorization Management Program (FedRAMP),[29] the European Union's General Data Protection Regulation (GDPR),[30]

---

[27] 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

[28] 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

[29] 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.

[30] 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/.

(continued...)

the Federal Information Processing Standard Publication (FIPS 140-2),[31] the International Organization for Standardization (ISO),[32] and the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR).[33] 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.[34] This allows customers to continuously monitor AWS security and compliance and have access to new audit reports. 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 simplify compliance with industry-specific security assurance requirements.

Customer scans of third-party service provider systems as contemplated by the proposed rules are not feasible.

Rule 10 suggests a Covered Entity review or scan service provider systems as part of a Covered Entity's obligation to detect vulnerabilities.[35] In practice, this is not feasible because Covered Entities control their own use of cloud, including the products, services, and configurations related to that use, while AWS controls the security protocols related to the underlying infrastructure and environment. As a result, there is no comprehensive "system" that a Covered Entity could review or scan, as the use and security posture of each Covered Entity may be different and dynamic, depending on their usage, security decisions, and risk tolerance.

---

[31] 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/.
[32] 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/.
[33] 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/
[34] 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/
[35] *id*. at 109-10.
(continued...)

To assist navigating this reality, AWS supports customer assessments and scans of their own use of AWS. This allows customers to conduct security assessments or penetration tests of their AWS infrastructure within "Permitted Services."[36] In some instances, AWS *requires* customers to perform scanning, penetration testing, file integrity monitoring, and intrusion detection.[37]

For the AWS environment, including its global infrastructure, AWS Security performs regular vulnerability scans using a variety of tools. External vulnerability assessments are conducted by an AWS-approved third-party vendor at least quarterly, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities.[38] In comparison, customer reviews and scans of the complete AWS environment would not be reflective of the customer's individual use or access to that environment. Further, thousands of customers attempting to perform technical assessments simultaneously may disrupt or interfere with AWS processes for scanning and updating vulnerabilities.

Reliance on AWS' external vulnerabilities assessments is a more practical, realistic and efficient approach to assurance. Standardizing the third-party service provider information to be included in reports and certifications as a substitute for scans or other invasive investigations can simultaneously yield higher quality, more consistent results and useful information, while reducing adverse impacts on customers and third-party service providers.

---

[36] AMAZON WEB SERVICES, AWS CUSTOMER SUPPORT POLICY FOR PENETRATION TESTING, https://aws.amazon.com/security/penetration-testing/ (last visited June 3, 2023).
[37] Required for all Amazon EC2 and Amazon ECS instances and applications.
[38] Control AWSCA-3.4

An encryption safe harbor incentivizes adoption of security leading practices.

Creating an encryption safe harbor offers one potential solution to the dual challenges of encouraging uptake of leading cybersecurity practices and limiting the potential for voluminous over-reporting of less severe incidents. Reducing such overreporting would allow the Commission and the investor community to focus on the most severe and materially harmful incidents. AWS supports the creation of an encryption safe harbor to expressly exclude encrypted data from incident notification requirements. This approach has the additional benefit of harmonizing the Commission's rule with existing state data breach notification rules.[39]

As of January 5, 2023, all new object uploads to Amazon Simple Storage Service (Amazon S3) are automatically encrypted at no additional cost to customers and with no impact on performance.[40] This creates a new base level of encryption to all new objects being uploaded that customers cannot disable.[41] Amazon S3 encrypts customer data at the object level as it writes it to disks in AWS data centers and decrypts it when customers access it. Server-side encryption (SSE) is the encryption of data at its destination by the application or service that receives it. AWS SSE-S3, relying on 256-bit Advanced Encryption Standard (AES-256), is automatically applied to all new buckets and to any existing S3 bucket that doesn't already have default encryption configured. AWS offers customers additional layers of security to data at rest in the cloud by providing scalable and efficient encryption features, including flexible key management, encrypted message queues for the transmission of sensitive data, and Application Programming Interfaces (APIs) integrating encryption and data protection with any service developed or deployed in an AWS environment.

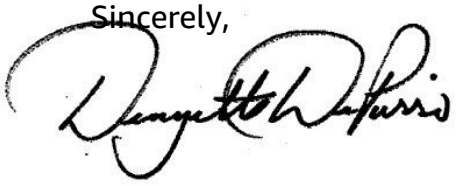
---

[39] *See, e.g.*, Cal. Civ. Code § 1798.82; N.Y. Gen. Bus. Law § 899-AA.
[40] AMAZON WEB SERVICES, *Protecting data using server-side encryption*, *in* AMAZON SIMPLE STORAGE USER GUIDE (Mar. 1, 2006), docs. aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html.
[41] *See* AMAZON WEB SERVICES, AMAZON S3 NOW AUTOMATICALLY ENCRYPTS ALL NEW OBJECTS, www.docs.aws.amazon.com/AmazonS3/latest/userguide/default-encryption-faq.html (last visited June 3, 2023) ("Can I disable encryption for the new objects being written to my bucket? No. SSE-S3 is the new base level of encryption that's applied to all the new objects being uploaded to your bucket. You can no longer disable encryption for new object uploads.").

* * *

AWS appreciates the opportunity to provide comments to the Commission on these proposals. Please contact me with questions regarding this letter, its suggestions, or recommendations. AWS appreciates the Commission's interest in inviting feedback on questions at the crossroads of cloud technology and financial services. On behalf of AWS, I invite the opportunity to meet and further discuss these approaches to cybersecurity, risk management, and incident response. I remain available to coordinate within AWS to support the Commission's work and understanding of cloud services within financial services.

Sincerely,



Denyette DePierro
US Financial Services Lead
AWS Public Policy
denyette@amazon.com