Tuesday, August 22, 2023

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

Filed electronically at: rule-comments@sec.gov

Re: File No. S7-07-23; *Regulation Systems Compliance and Integrity*; Release No. 34-97143 (RegSCI Proposal)

Dear Ms. Countryman:

Amazon Web Services, Inc. (AWS)[1] appreciates the opportunity to provide comments to the Securities and Exchange Commission (Commission) on proposed revisions to Regulation Systems Compliance and Integrity (RegSCI). AWS appreciates the Commission's recognition of the many benefits third-party service providers bring to SCI entities and of the "growing role third-party service providers are playing with respect to SCI systems and indirect SCI systems."[2]

As a cloud service provider (CSP), AWS invites an ongoing dialogue with the Commission to bring a third-party service provider perspective to cybersecurity oversight, and would welcome a deeper discussion of the responses included in this submission.

---

[1] To learn more about the impact of cloud services on the U.S. economy, AWS commissioned an independent consultancy, Public First, to undertake quantitative research to understand the use of and benefits created by cloud services across the U.S., with a particular focus on Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) forms of cloud services. Public First conducted a survey of over 3,000 U.S. businesses across regions and industries, including over 1,500 cloud users. PUBLIC FIRST, THE IMPACT OF CLOUD SERVICES IN THE UNITED STATES, https://cloudimpactus.publicfirst.co/ (last visited Aug. 16, 2023).

[2] RegSCI proposal at 112.

In 2006, AWS began offering information technology infrastructure—now commonly known as cloud computing.[3] Today, AWS provides reliable, secure, scalable, agile, and low-cost cloud services 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 services enable rapid, cost-effective innovation while enhancing customer security and resilience. AWS consistently implements processes to protect customer data, and enhance the security and resilience of cloud computing and the information technology cybersecurity infrastructure.

Cloud services create "cost efficiencies, automation, increased security, and resiliency"[4] and allow SCI entities to "reengineer or otherwise update their systems and applications to run even more efficiently"[5]—a policy perspective echoed in the U.S. Department of Treasury's (Treasury) report, The Financial Services Sector's Adoption of Cloud Services.[6] As a third-party service provider to the financial services sector, AWS supports customers in asset management, banking, capital markets, insurance, and payments, among others.[7] AWS provides financial firms secure,

---

[3] 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. The 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 1 n.1 (2020), https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-46a.pdf (citing PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COM., THE NIST DEFINITION OF CLOUD COMPUTING 2 (Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf).

[4] RegSCI proposal at 372.

[5] *Id*.

[6] U.S. DEP'T OF THE TREASURY, THE FINANCIAL SERVICES SECTOR'S ADOPTION OF CLOUD SERVICES 21 (Feb. 2023), https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf ("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.").

[7] In addition to financial services, AWS' regulated customers also operate across a range of industries, including healthcare, education, government, transportation, telecommunications, and energy. *See AWS Services in Scope by Compliance Program*, AMAZON, https://aws.amazon.com/compliance/services-in-scope/.

resilient global cloud services to innovate, enhance customer experience, differentiate for growth, and adapt to future technology needs.[8] As AWS customers, these firms have access to over two-hundred AWS services for computing, storage, databases, networking, analytics, machine learning and artificial intelligence, security, and application development, deployment, and management.[9]

This letter is intended as a companion to the AWS comment letter submitted June 5, 2023 (June 5 letter) in response to the Regulation S-P, Rule 10, and Cybersecurity Risk Management for Investment Advisers proposals.[10] As detailed in that prior letter, AWS urges the Commission to consider alignment and regulatory integration as it evaluates the totality of its proposed cybersecurity framework. Defragmentation and integration are essential within financial services supervision and across the Commission's rules and regulations. As noted in the June 5 letter,[11] cybersecurity and resilience are critical components of cloud services.

---

[8] *See Customer Success Stories*, AMAZON, 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-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 (AWS case studies of global financial services customers).

[9] *Id*.

[10] In Commission Chair Gensler's comments to the U.S. House Financial Services Committee on April 18, 2023, he was asked by Chair Patrick McHenry, Representative Gottheimer, and Representative Peterson allowing adequate time for industry feedback. Chair Gensler responded to Representative Gottheimer saying, "we have a formal end to a comment period. But then we get comments after that, and we take meetings after that, and we engage actively with trade associations and market participants." He further noted, "we also often consider comments well beyond [the comment deadline] and continue to receive comments. On average, it takes 12 to 15 months from proposal to considering an adoption." Chair Gensler had a similar exchange on September 14, 2022 in the Senate Banking Committee with Senator Warner, saying "We benefit from the public comment. And I would say, we have a long tradition, regardless of what the comment period is, 60 days or whatever the comment period is, when comments come in after the comment period, we still, the staff considers it. We write it up. We put it in…Generally, on average it takes a year, year and a half to finalize these things. So, I encourage people to continue." Gary Gensler, Chair, Commission, Testimony before the United States House of Representatives Committee on Financial Services (Apr. 18, 2023), https://www.sec.gov/news/testimony/gensler-testimony-house-financial-services-041823.

[11] Letter from Denyette DePierro, U.S. Fin. Servs. Lead, AWS Pub. Pol'y, to Vanessa Countryman, Secretary, Commission (June 5, 2023), https://www.sec.gov/comments/s7-06-23/s70623-208239-420942.pdf.

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 between the public and private sectors is essential to ensure a secure and level playing field for all market participants.[12] Harmonization supports the larger goal of fostering a defragmented, consistent, and fair regulatory framework as the foundation of a thriving, innovative financial sector.[13]

The proposed changes to RegSCI are part of a global policy trend focusing on the security and resilience of the financial services sector. Recent regulatory proposals, administrative actions, policy recommendations, and legislation

---

[12] 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. *See Market Participants*, SEC: INTRODUCTION TO INVESTING, https://www.investor.gov/introduction-investing/investing-basics/how-stock-markets-work/market-participants For technical information on Market Participants, visit http://www.sec.gov/divisions/marketreg/mrclearing.shtml.

[13] Harmonization is listed as a priority in the recently released U.S. National Cybersecurity Strategy. The Strategy clarifies 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.*

The White House also recently released a Request for Information (RFI) on Cyber Regulatory Harmonization. In the RFI announcement, the White House reiterated that "[w]hen cybersecurity regulations of the same underlying technology are inconsistent or contradictory – or where they are duplicative but enforced differently by different regulators – consumers pay more, and our national security suffers." The White House expressed concern that "Duplicative regulation leads to companies focusing more on compliance than on security" and called for "[h]armonizing baseline regulatory requirements" to "produce better security outcomes at lower costs." Press Release, The White House, Fact Sheet: Office of the National Cyber Director Requests Public Comment on Harmonizing Cybersecurity Regulations (July 19, 2023); *see also Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations*, 88 Fed. Reg. 55694 (Office of the Nat'l Cyber Dir. Aug. 16, 2023) (calling for "establishing cybersecurity regulations to secure critical infrastructure where existing measures are insufficient, harmonizing and streamlining new and existing regulations, and enabling regulated entities to afford to achieve security" and defined harmonization to mean "a common set of updated baseline regulatory requirements that would apply across sectors").

includes the 2021 Computer-Security Incident Notification Rule,[14] the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),[15] pending incident response, cybersecurity, and business continuity rules from the Commodity Futures Trading Commission (CFTC),[16] revisions to the New York Department of Financial Services' Cybersecurity Regulation,[17] final guidance on third-party risk management from the Federal Deposit Insurance Corporation, Federal Reserve Board of Governors, and the Office of the Comptroller of the Currency (OCC),[18] proposed Financial Stability Board 'toolkit' on Third Party Risk Management,[19] and the National Institute for Standards and Technology (NIST) Cybersecurity Framework 2.0.[20] This cybersecurity policy trend is not only global, significant, and dynamic but also increasing in the number of promulgating jurisdictions and the speed of rulemaking.

There also is a concurrent emerging trend towards regulatory coordination. For example, in a June 2023 speech, CFTC Commissioner Romero announced the "Five Pillars of Cyber Resilience."[21] This approach relies on proportionate, tailored, flexible rules commensurate with risk; aligns with accepted standards and best practices, including International Organization for Standardization (ISO) standards and the NIST Cybersecurity Framework; and seeks to harmonize with other sector requirements.[22]

---

[14] *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).

[15] Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, 136 STAT. 49, 1038-59 (2022).

[16] *See 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); *Derivatives Clearing Organizations Recovery and Orderly Wind Down Plans; Information for Resolution Planning*, 88 Fed. Reg. 48968 (proposed June 7, 2023) (to be codified at 17 C.F.R. pts. 39, 190).

[17] Revised Proposed Second Amendment to 23 NYCRR 500 (proposed June 28, 2023), https://www.dfs.ny.gov/system/files/documents/2023/06/rev_rp_23a2_text_20230628.pdf.

[18] BD. OF GOVERNORS OF THE FED. RSRV. SYS., FDIC, OCC, TREAS., INTERAGENCY GUIDANCE ON THIRD-PARTY RISK MANAGEMENT (June 1, 2023), https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53a.pdf.

[19] *Id*.

[20] NIST RELEASES CYBERSECURITY FRAMEWORK 2.0 DRAFT & IMPLEMENTATION EXAMPLES, NIST COMPUT. SEC. RES. CTR. (Aug. 8, 2023), https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft.

[21] Christy Goldsmith Romero, CFTC Comm'r, Advancing from Incident Response to Cyber Resilience at FIA International Derivatives Expo Conference (June 20, 2023) (transcript available at https://www.cftc.gov/PressRoom/SpeechesTestimony/oparomero9).

[22] *Id.* ("In order to advance from incident response to cyber resilience, I believe that there are five pillars of a cyber resilience framework: (1) A proportionate and appropriate approach: Operational resilience is not a one-size-fits-all approach. For a resilience strategy to work, it must fit each organization. It must be tailored, flexible, and commensurate with the risks faced. (2) Following generally accepted standards and best practices: There are generally accepted standards designed to promote cyber resilience. These include standards and best practices by NIST's Cybersecurity Framework, and the

As summarized, each of these policy efforts overlap in intent and scope with the Commission's proposals and could subject third-party service providers and their customers to multiple overlapping and related regulations, including RegSCI. This potential overlap risks the creation of competing and conflicting obligations for third-party service providers and their customers. Rulemaking should evaluate existing law and standards, consider the quickly evolving regulatory landscape, and address how the Commission's approach will align with cybersecurity, incident reporting, business continuity requirements, guidance, and proposals emerging from other agencies and entities.

AWS urges the Commission to consider the proposal cautiously as new rules and regulations are adopted throughout the financial sector. Accordingly, AWS reiterates the request made in the June 5 letter[23] strongly encouraging the Commission to work closely with Cybersecurity and Infrastructure Security Agency (CISA), Treasury, and the federal banking agencies to ensure a coordinated national approach to cybersecurity and operational resilience in the financial services sector.

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

Relying on widely adopted and globally respected standards, frameworks, and guidelines would ensure that RegSCI responds to evolving threats and technological change. Often developed in close collaboration with private sector experts, the standard-setting organizations, like NIST and ISO, host robust working groups and quickly integrate public comments and necessary revisions into leading edge standards.

International Organization for Standards (ISO). Among best practices are training, review of resilience plans, and testing. (3) Elevating responsibility through governance: Building resilience requires elevating responsibility for resilience to those who make strategic decisions about the business. It's a business risk if companies do not have operational resilience plans properly tailored to their risks. That means putting those plans on the executive agenda. (4) Building resilience to third-party risk: Operational resilience cannot be achieved without ensuring that a third party's servicer's door is secured against cyber criminals. Generally accepted standards discuss heightened scrutiny where the third party is deemed "critical." (5) Avoiding reinventing the wheel—instead leveraging the important work already done in this space: CFTC recognizes that some CFTC entities are also subject to the rules promulgated by the federal banking agencies and will seek to harmonize their requirements as appropriate.").

[23] Letter from Denyette DePierro to Vanessa Countryman, *supra* note 11.

These standards, frameworks, and guidelines include the NIST Cybersecurity Framework,[24] the NIST Control Objectives for Information and Related Technologies,[25] the ISO standards,[26] the Center for Internet Security (CIS) Critical Security Controls,[27] the OCC's Cybersecurity Supervision Work Program,[28] CISA's anticipated Cybersecurity Performance Goals (CPG)[29] for the financial services sector, as well as the Cyber Risk Institute's Cybersecurity and Cloud Profiles,[30] which are mapped to global financial services regulations, including the Commission's RegSCI.

The optimum supervisory posture supports robust, sector-wide cybersecurity, and by extension, the optimum approach to RegSCI would incorporate and rely on these leading cybersecurity standards. 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.

---

[24] *Cybersecurity Framework*, NIST, https://www.nist.gov/cyberframework. We note that NIST has proposed an updated framework, NIST Cybersecurity Framework 2.0, which is currently available for public comment before its finalization in 2024. *See supra* note 20. We expect this framework will again be widely adopted by the financial service sector and others.

[25] *Security and Privacy Controls for Information Systems and Organizations*, NIST COMPUT. RES. CTR. (Sept. 2020), https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[26] INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/home.html (last visited Aug. 16, 2023).

[27] Critical Security Controls Version 8, CTR. FOR INTERNET SEC. (May 2021), https://www.cisecurity.org/controls/v8.

[28] OCC BULLETIN 2023-22, CYBERSECURITY: CYBERSECURITY SUPERVISION WORK PROGRAM (June 26, 2023), https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-22.html; *see also Cybersecurity Supervision Work Program*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.gov/topics/supervision-and-examination/bank-operations/bit/cybersecurity-supervision-work-program-overview.html#:~:text=The%20Cybersecurity%20Supervision%20Work%20Program%20%28CSW%29%20is%20a,%28OCC%29%20risk-based%20bank%20information%20technology%20%28BIT%29%20supervision%20process ("The Cybersecurity Supervision Work Program (CSW) is a component of the Office of the Comptroller of the Currency's (OCC) risk-based bank information technology (BIT) supervision process. The CSW provides high-level examination objectives and procedures that are aligned with existing supervisory guidance and the National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF).").

[29] Cross-Sector Cybersecurity Performance Goals, CISA, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (last visited Aug. 16, 2023).

[30] *The Profile*, CYBER RISK INST., https://cyberriskinstitute.org/the-profile/; *see also* OCC Bulletin 2023-22, *supra* note 28, at 1 (noting "the OCC continues to encourage, but does not require, the use of standardized approaches to assess and improve cybersecurity preparedness" and citing the Cyber Risk Institute profile).

III. AWS encourages a pragmatic, data-driven, principles-based approach to cybersecurity that considers appropriate timelines, triggers, and technology.

In its June 2023 paper on regulatory approaches to cybersecurity, the Financial Stability Institute observed that "[t]he risk exists that regulation becomes too prescriptive, so that it falls behind both the constantly evolving threat from cyber risk and advances in cyber risk management."[31] The paper suggests countering prescriptiveness with an approach combining broad resilience principles with baseline requirements. This approach focuses more on "'what expectations to achieve' and less on 'how to achieve them.' It supports a regulatory framework that is adequately flexible to be adapted to the dynamic and evolving nature of cyber risk while setting clear supervisory expectations for the core aspects of governance and risk management that enhance cyber resilience."[32] Regulations prescribing specific technology, recovery goals,[33] or contractual language are likely to become rapidly outdated and ineffective.

IV. Not expanding the definition of "systems intrusion" to include significant attempted unauthorized entries.

Under Rule 1002 of RegSCI, a "systems intrusion" is "any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity."[34] As the Commission notes, under this definition, "the term systems intrusion only applies to 'successful' intrusions" and "the intrusion is limited to events that result in an intruder entering into the SCI entity's SCI systems or indirect SCI systems."[35]

The RegSCI Proposal would expand the definition of systems intrusion to "include any significant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity."[36] The Commission proposes to require SCI entities to determine whether an attempted unauthorized entry is "significant." Such a determination requires a thorough fact-based analysis that will, together with the requirement to provide immediate notification,

---

[31] JUAN CARLOS CRISANTO, JEFFERSON UMEBARA PELEGRINI AND JERMY PRENIO, FIN. STABILITY INST., BANK OF INT'L SETTLEMENTS, FSI INSIGHTS ON POLICY IMPLEMENTATION NO 50, at 12 (2023).
[32] *Id.*
[33] *Id.* ("Mandating a specific recovery time is another example where regulators need to be careful how banks go about implementing it. The aim is to prevent the lengthy disruption of critical financial operations, but an excessively stringent and rigid recovery time may prove counterproductive if this comes at the expense of banks' ability to thoroughly check that all their systems are no longer compromised.").
[34] RegSCI Proposal at 20.
[35] *Id*. at 131.
[36] *Id*. at 134.

require SCI entities and technology service providers to prioritize investigating and reporting circumstances around unsuccessful attempts with the same urgency as successful active system intrusions, and potentially force organizations to divert valuable security resources towards attempts leaving less capacity to respond to actualized risks.

V. Permitting coordinated, standardized solutions for audit, testing, and assessments ensures high-quality, consistent and efficient evaluation while reducing the potential for operational disruption.

The RegSCI Proposal includes various changes related to SCI entities' obligations to oversee and manage their third-party providers. AWS supports appropriate due diligence and third-party risk management and believes that SCI entities and their third-party service providers should be permitted to perform such oversight and management in a manner that satisfies RegSCI's intent while also preserving the security of a multi-tenant environment.

There is growing global recognition of the value of "pooled audits," reliance on independent third-party audit reports, and other audit efficiencies for third party assessments. In June 2023, the Bank of International Settlements (BIS) acknowledged the utility of consolidated audit procedures, stating:

> [s]ome [financial institution]s rely on third-party assurance reviews, such as service organi[z]ation controls (SOC) reviews, penetration tests, and vulnerability assessments, to understand [a cloud service provider]'s control environment. Other [financial institution]s are combining their resources to conduct or hire auditors to conduct "pooled" audits and certifications or are considering doing so.[37]

In its February 2023 white paper, the Treasury acknowledged that "intensive in-person audits are challenging to accommodate at scale while maintaining the security of the multi-tenant environment,"[38] and noted its support for "alternative approaches to one-to-one audits like pooled audits, certifications, or real-time updates to customers[]" and "efforts that could yield efficiency gains for both CSPs and financial institutions without compromising outcomes."[39]

---

[37] JUAN CARLOS CRISANTO ET AL., *supra* note 31, at 22.
[38] U.S. DEP'T OF THE TREASURY, *supra* note 6.
[39] U.S. DEP'T OF THE TREASURY, *supra* note 6, at 5.

The Monetary Authority of Singapore similarly observed in its 2021 advisory on public cloud adoption that "[financial institutions (FIs)] may adopt a risk-based approach in exercising the necessary due diligence, such as relying on 'pooled audits' that are performed by independent and qualified auditors jointly engaged by the FIs or clients using the same cloud service,…provision of reputable audit reports that evidence compliance with recogni[z]ed risk management standards; and/or…provision of reputable industry certifications for IT security, resiliency and services."[40]

AWS agrees with these authorities and strongly encourages the Commission to permit and encourage SCI entities to rely on consolidated or *pooled* testing and audit, third-party audit reports, and other efficiencies for SCI entities and third-party service providers.

VI. AWS provides state-of-the-art operational resilience and minimizes points of failure.

As a global cloud service provider, AWS invests in people, processes, and technologies to maximize availability—the uninterrupted provision of cloud services—and to enhance resiliency—the ability to resist and recover from failures. Cloud solutions can improve resiliency for companies compared to on-premises solutions. For smaller companies, highly available, resilient, and secure on-premises solutions are complicated and costly to design and maintain. By contrast, cloud providers invest substantially more overall in maintaining and securing their facilities than most individual customers would invest to protect their own on-premises data centers.

a. Cloud computing enhances resiliency for all customers without creating a single point of failure.

On-premises infrastructure typically involves just one or a few data centers. But cloud services offer a global cloud infrastructure with built-in redundancy to minimize risks of outages. The AWS cloud is organized into 31 Regions, 99 sub-regions called Availability Zones, and at least one—but typically multiple—physical data centers within each Availability Zone. Regions are independent and isolated from each other, so a service outage has never affected multiple AWS Regions simultaneously. Within each Region, Availability Zones are located miles apart from each other and operate independently. Each Availability Zone has independent grid power,

[40] Letter from Tommy Tan, Director & Head (Division I), Monetary Authority of Singapore to Chief Executive Officers of All Financial Institutions (June 1, 2021), https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Cloud-Advisory.pdf.

backup power, and physical security, as well as redundant network connections to reduce the risk of disruptions from power outages and natural disasters. This design minimizes the risk of data loss from disruptions or outages, especially compared to the inherent vulnerability of a single on-premises data center.

Customers can benefit from redundant cloud infrastructure without creating the risk of industry-wide outages from shared CSP use. In the rare case of an outage, customers might not be impacted because they store data and run applications in a Region that was not affected, or because they operate in multiple Regions at the same time. Other customers might experience brief disruptions. Even in those rare circumstances, each impacted customer can recover quickly according to its own disaster-recovery plan.

b. Customers can use different cloud designs to enhance availability and resiliency.

Some AWS customers choose to operate primary and secondary virtual private clouds located across two geographically diverse Regions, with each Region having three Availability Zones. This provides for multiple levels of redundancy in addition to an on-premises data center as a traditional backup to the backup. Another option available to customers is AWS Outposts. With Outposts, customers use servers that they do not share with any other AWS customer and may be kept on premises, while still enjoying the benefits of cloud services such as active security monitoring and greater control over access to data. They can use multiple Outposts running in separate locations and in different AWS Regions to maximize availability, resiliency, and disaster recovery.

On top of this redundant and resilient physical infrastructure, AWS also offers state-of-the-art software capabilities that automatically address failures. AWS storage and database services automatically replicate data across multiple Availability Zones. This means that a customer's data is redundantly stored and fully available even if an entire data center or Availability Zone experiences an outage. AWS storage and database services also enhance a customer's ability to recover from accidental deletions or application failures. For example, Amazon S3 Standard data storage is designed for 99.999999999% durability. This means that a customer storing 10 million objects could lose just 1 every 10,000 years. While minimizing outages, the AWS cloud helps customers quickly recover and return to normal operations in the rare case an outage occurs. If a failure occurs, customers can create processes to move traffic from the affected area and continue operating from another part of the AWS network.

Customers also rely on AWS Health,[41] a service providing real-time information around availability problems, and use this information in decision making to shift traffic to avoid service interruptions.

c. AWS provides features, tools, and guidance to help improve resiliency.

AWS' Well-Architected Framework helps customers build secure, high-performing, resilient, and efficient infrastructure for their applications. The free Well-Architected Tool helps compare the security and resiliency of data to the latest best practices. Customers can also assess the resilience of their applications and receive actionable recommendations to improve. Finally, AWS helps customers prepare for disasters and develop recovery plans. One AWS service simulates outages so customers can experiment to discover and address vulnerabilities. Customers can participate in AWS workshops to help design, manage, and test applications that require timely and reliable disaster recovery to meet stringent regulatory requirements. Further, different customers choose different recovery plans, further minimizing the risk that a rare outage will have industry-wide impact.[42]

VII. Multicloud and on-premises backup are costly, complex, and impractical.

The Commission is proposing to revise Rule 1001(a)(2)(v) to require SCI entities to have policies and procedures designed to address the unavailability of third-party providers supporting critical SCI systems. AWS supports the view that "it is appropriate to require SCI entities to have even more robust policies and procedures with respect to any third-party provider that supports such [critical SCI] systems."[43] However, AWS disagrees with the Commission's commentary that "an SCI entity could consider if use of a CSP for its critical SCI systems also warrants maintaining an 'on-premises' backup data center or other contingency plan" to address the unavailability of third-party providers.[44] Many global authorities note that multi-vendor, multicloud failover entails significant cost and complexity that can be detrimental to overall efforts to improve uptime, reduce risks, and improve security and resiliency.

---

[41] *Service Health*, AMAZON: AWS HEALTH DASHBOARD, https://health.aws.amazon.com/health/status (last visited Aug. 16, 2023).

[42] Customers can choose from a range of disaster-recovery plans enabling quick recovery and return to normal operations after a failure, including (1) a "pilot light" plan that copies data and applications into a second Region and resumes normal operations within tens of minutes; (2) a "warm standby" plan that resumes operations in a matter of minutes; and (3) for the most business-critical work, a "multi-site active/active" plan that offers near-zero downtime in the event of a failure. *Id.*

[43] RegSCI Proposal at 118.

[44] *Id.* at 119.

For example, the Treasury noted in its February 2023 white paper:

> …[w]hile many financial institutions can increase resilience by operating in multiple regions of the same CSP, few experts believe that complex use cases can be developed to support seamless failover from one CSP environment to a different CSP environment. Reasons include the inherent differences among service offerings, the associated complexity of designing across multiple cloud environments, and the need to hire multiple staff familiar with various environments.[45]

The Treasury described multicloud (called "multi-vendor, single-use case deployment" in the report)[46] as an "idealized solution" that is "impractical," and "inadvisable."[47] The report describes the financial sector's consensus that multicloud is "too technically complex" and that the resulting operational risk is too high, "given the costs, staffing, and complexity involved . . . particularly the complexity associated with identifying and managing risk across multiple cloud environments."[48] The Monetary Authority of Singapore has made similar observations about multicloud saying, "FIs should be cognizant of the added complexity of operating in a multi-cloud environment, such as having adequate resources and appropriate expertise in securing and managing the use of different public cloud services and ensuring the consistent enforcement of policies."[49] In the Treasury report, which summarized interviews of a cross-section of cloud stakeholders, financial institutions observed that running the same application on two or more CSPs simultaneously "can be impractical."[50] Further, they reported that "monitoring threats, like unauthorized activity, were made easier when all critical information systems were running on the same platform."[51]

---

[45] U.S. DEP'T OF THE TREASURY, *supra* note 6, at 56.
[46] U.S. DEP'T OF THE TREASURY, SUPRA NOTE 6, AT 26.
[47] U.S. DEP'T OF THE TREASURY, SUPRA NOTE 6, AT 56.
[48] U.S. DEP'T OF THE TREASURY, SUPRA NOTE 6, AT 56.
[49] LETTER FROM TOMMY TAN TO CHIEF EXECUTIVE OFFICERS OF ALL FINANCIAL INSTITUTIONS, SUPRA NOTE 40.
[50] U.S. DEP'T OF THE TREASURY, *supra* NOTE 6, at 56.
[51] U.S. DEP'T OF THE TREASURY, *supra* note 6, at 56.

Concentration Risk

One of the questions raised in the Treasury report is whether to extend the financial services analysis of concentration risk to third-party risk management. The Treasury report mentions hypothetical scenarios about the impact of system failure or data breach, but also clarifies that "the mere presence of large CSPs is not necessarily an issue for the financial sector's operational resilience. Evaluating the operational risks that could arise from concentration in cloud services depends on how firms use and design these services."[52]

In its April 2023 report, Cloud Adoption in the Financial Sector and Concentration Risk, the Program on International Financial Systems (PIFS) found that "…it is not necessarily the case that [concentration] risks could be avoided if FIs were to rely or continue to rely on traditional IT infrastructure…*thus, the critical question is not how to eliminate concentration risk, but how to manage or mitigate it.*"[53] The PIFS report further acknowledges the capacity of CSPs and customers to mitigate the risk. CSPs "…mitigate the possibility of any single point of failure in their own infrastructure…[by] spreading infrastructure across different 'availability zones' and regions."[54] Concurrently, customers "…can distribute processes and data across a cloud provider's different availability zones or regions, allowing them to build applications that can be online even if a particular data center or region experiences a disruption."[55]

Any attempt to develop a risk management approach to identify and mitigate potential concentration requires a definition of concentration specific to the provision of technology services. Currently, there are several public and private sector efforts to dive deep into the concentration analysis. Among them is the ISO/International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1/Subcommittee (SC) 38/Working Group (WG) 5, *Data in cloud computing and related technologies*,[56]

---

[52] U.S. DEP'T OF THE TREASURY, *supra* note 6, at 57.

[53] HAL SCOTT, JOHN GULLIVER, HILLEL NADLER, AND JON ONDREJKO, PROGRAM ON INT'L FIN. SYS., CLOUD ADOPTION IN THE FINANCIAL SECTOR AND CONCENTRATION RISK 13-14 (2023), https://s9y8d2p9.stackpathcdn.com/wp-content/uploads/2023/04/PIFS-Cloud-Adoption-in-the-Financial-Sector-and-Concentration-Risk-04.19.2023.pdf

[54] *Id*. at 15.

[55] *Id.*

[56] *Cloud computing and distributed platforms*, ISO, https://www.iso.org/committee/601355.html (last visited Aug. 16, 2023).

and the Treasury-convened Cloud Executive Steering Group[57] and its supporting public/private sector working groups. We encourage the Commission to engage with this work and other private and public sector dialogs before deciding if further regulations related to third party risk management and concentration concerns are necessary.

* * *

AWS appreciates the opportunity to provide comments to the Commission on the RegSCI Proposal. We welcome the opportunity to discuss our views with you in greater detail.

Sincerely,

Denyette DePierro

Financial Services Lead, Public Policy

denyette@amazon.com

[57] Press Release, U.S. Dep't of the Treasury, U.S. Department of the Treasury Kicks Off Public-Private Executive Steering Group to Address Cloud Report Recommendations (May 23, 2023), https://home.treasury.gov/news/press-releases/jy1503.