Google Cloud

June 13, 2023

Submitted via email to rule-comments@sec.gov (File S7-07-23)

U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090.

Re: Regulation Systems Compliance and Integrity (SCI) Proposal

On March 15, 2023, the Securities and Exchange Commission ("Commission") proposed changes to Regulation Systems Compliance and Integrity ("SCI"). These proposed changes to Regulation SCI, which provides the Commission with oversight of the core technology of key U.S. securities markets entities (SCI entities), seek to "take account of the evolution of technology and trading since the regulation's adoption in 2014 and to continue to help ensure the capacity, integrity, resiliency, availability, and security of the technology infrastructure of the U.S. securities markets."

The Regulation SCI proposal includes a range of provisions related to third party providers, including cloud services providers. As a provider of cloud services to the financial industry, Google Cloud welcomes the Commission's proposals. The interest in protecting the technology infrastructure of the U.S. securities markets is one that is strongly shared by Google Cloud and is an area in which Google Cloud has extensive experience. We appreciate the opportunity to provide comments on the Regulation SCI proposal with this experience in mind.

I. Observations and Comments

As noted above, effective cybersecurity and system safeguards, including with respect to incident response and notification, are critical for the financial markets and services industry and the regulators tasked with supervising regulated intermediaries. We urge that the following principles and considerations inform the regulatory effort to modernize these requirements.

1. **Technology Neutrality.** In its commentary, the Commission uses language that may be interpreted to suggest that cloud service providers ought to be subject to heightened scrutiny under Regulation SCI. Specifically, the Commission states "[i]n deciding whether to utilize a CSP, an SCI entity generally should take into account the various factors it would as with any other third-party providers. However, given the degree to which CSP services may be integral to the operation of SCI systems, *SCI entities generally should examine closely any potential relationship and utilization of CSP services*." (Emphasis added.) Elsewhere, the

Commission notes that a "third-party provider [risk] assessment may be particularly relevant with respect to CSPs utilized by SCI entities."

We urge the Commission to make clear that it continues to take a technology neutral, and risk-based, approach to ensuring that the nation's securities markets are protected. In the recent report entitled "The Financial Services Sector's Adoption of Cloud Services," the U.S. Treasury Department notes that financial institutions ("FIs") utilize a broad range of cloud services "from video conferencing and collaboration software to banking and trading platforms that support internal operations and business line functions." Further, the Treasury report notes that one of the primary drivers for the financial sector's migration to cloud is "[t]he potential for increased resilience to physical and cyber incidents, with the use of multiple data centers or regions from the same CSP and broader use of encryption and zero trust models."

As the Treasury report acknowledges, there is no single use case for cloud services in the financial services sector, nor single risk profile. Moreover, as Treasury notes, cloud may be selected precisely because it presents *less* risk – and more potential for safeguarding capacity, integrity, resiliency, availability, and security – than alternatives. In applying third-party risk considerations under Regulation SCI and ensuring that they can continue to meet their obligations under the regulations, financial institutions should apply the same rigor and care with assessment of all third service party providers, including cloud service providers, taking into account their specific role and function within the institution's business operations.

2. **Definition of Systems Intrusion.** The Regulation SCI proposal expands the definition of systems intrusion to include "[s]ignificant *attempted* unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria." (Emphasis added.) The Commission states that:

> [This] third prong is intended to capture unsuccessful, but significant, attempts to enter an SCI entity's SCI systems or indirect SCI systems. The Commission recognizes that it would be inefficient, inappropriate, and undesirable (for both SCI entities as well as the Commission and its staff) to require that all attempted entries be considered systems intrusions. Rather, the Commission is seeking to include only attempts that an SCI entity believes to be significant attempts to its systems, even if successfully prevented.

We urge the Commission to reconsider making attempted but unsuccessful attempts subject to the obligations in Regulation SCI applicable to systems intrusions. One such obligation is the requirement to take corrective action. However, in the case of unsuccessful attempts,

there is no corrective action that can be taken. Therefore, expanding the definition to include attempts adds little benefit in this regard.

In addition, a set of notification obligations applies with respect to systems intrusions, including the requirement to provide "immediate" notification to the Commission "upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event [including a systems intrusion] has occurred." Additional reporting obligations apply even to SCI events, including systems intrusions, ultimately determined to have no or *de minimis* impacts.

This expansion of notification and reporting obligations could have significant unintended consequences. An important aspect of an effective incident response process is ensuring that true positives/actual incidents are promptly flagged to affected customers (and subsequently to regulators, where necessary) and that these are not drowned out by false positives/non-material incidents. This helps service providers, FIs, and, ultimately, regulators focus on the incidents that matter and not expend resources on false or *de minimis* matters.

As the Commission notes, the fact that an event has not resulted in actual information/systems harm is often evidence that the applicable controls are operating as intended. Reporting of such events would significantly increase the operational burden on all involved parties, including financial institutions (who would be receiving excessive volumes of non-actionable information), without a clear benefit. This is likely to distract FIs from true incidents and, at worst, could itself lead to heightened security risks by compromising live investigations of as yet unconfirmed incidents.

With respect to more generalized threats that do not materialize, we and many others in the financial services industry participate in voluntary fora for information sharing about threats and how to respond to them.[1] These fora are important and should be considered, instead of incident notification, for purposes of raising general industry awareness and sensitivity.

Retaining the focus of incident reporting on events that are actualized and have a real impact would not only keep precious time and resources properly targeted, but it would also serve to harmonize regulatory approaches across the financial sector. We note in that regard that the Federal banking agencies in the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers have adopted the following definition: "[c]omputer-security incident is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."

[1] For example, Google Cloud joined FS-ISAC's Critical Providers Program in March 2023 to advance this objective.

3. **Third-Party Service Provider Considerations & Contracts.** We applaud the Commission's recognition that third-party service providers, including CSPs, are playing an increasingly important role in supporting and enhancing financial markets. We further agree that specific attention should be focused on ensuring that regulatory expectations are clear and consistent with respect to providers' role in ensuring that FI customers are able to meet requirements under the proposals.

   To this end, contracts are important tools both for (a) validating the capabilities of a service provider upfront, as well as (b) risk management during the life of the service relationship. We recognize the Commission's rationale in proposing a program to manage and oversee third-party providers that include initial and periodic contract reviews for consistency with the SCI entity's obligations under Regulation SCI. However, we are concerned that some of the examples provided in the Commission's commentary may, if followed, create unnecessary barriers to cloud adoption.

   In particular, the Commission suggests that "[t[he SCI entity may want to consider and, if appropriate, negotiate provisions that provide priority to the SCI entity's systems, such as for failover and/or business continuity and disaster recovery ("BC/DR") scenarios, if needed to meet the SCI entity's obligations under Regulation SCI." This proposal is not compatible with all service models. In the restoration of services, public CSPs focus on bringing up their services safely with respect to customer data and workload integrity overall. Due to the shared tenancy nature of public cloud services, it is not generally possible to prioritize one customer over another. Further, to address customer and regulator expectations of privacy and security, by design, the CSP does not have visibility into the exact identity or industry of the customers on our systems. Instead of seeking to negotiate terms requiring a public CSP to prioritize them during recovery, SCI entities should assess if the CSP's technical resilience and applicable recovery processes together with the SCI entitiy's chosen architecture provide the SCI entity what it needs to meet its obligations under Regulation SCI in respect of BC/DR.

   We also urge the Commission to consider making any new obligations with respect to contracting forward looking so as not to disrupt contracts already in existence by requiring renegotiation. In considering timeframes for implementation, as well, the Commission should give due regard to the extensiveness of the requirements and the reasonable time that will be needed for new commercial contractual provisions to be negotiated in line with them.

   Last, the Commission states that, as part of the program to manage and oversee third-party providers, SCI entities must conduct "analyses of third-party provider concentration." In its commentary, the Commission states that "[i]n performing this risk-based assessment, SCI entities would be required to consider third-party provider concentration, which would help

ensure that they properly account and prepare contingencies or alternatives for an overreliance on a given third-party provider by the SCI entity *or by its industry*." (Emphasis added) While considerations of an SCI entity's own concentration of workloads with a particular provider may be useful and appropriate from a resiliency standpoint, we caution against requiring an industry assessment. It is unclear how an SCI entity would come by such industry information. Certainly, having SCI entities seek out information from providers about other industry customers as a condition of doing business could have undesirable impacts, such as potentially exposing business proprietary information of competitors to each other. Accordingly, we recommend that the Commission focus this requirement on the SCI entity's own workloads.

4. **Business Continuity and Disaster Recovery Testing:** The Commission provides that "[b]ecause the Commission believes that some third-party providers may be of such importance to the operations of an SCI entity, the Commission is proposing to include certain third-party providers in the BC/DR testing requirements of Rule 1004." In particular, the Commission states that "the Commission believes it likely that, for an SCI entity that utilizes a cloud service provider for all, or nearly all, of its operations, such CSP would be of such importance to the operations of the SCI entity and the maintenance of fair and orderly markets in the event of the activation of the SCI entity's BC/DR plans that it would be required to participate in the BC/DR testing required by Rule 1004."

   We recognize fully the importance of BC/DR testing. As a CSP, Google tests our own BC/DR plans at least annually and shares information about the results of those tests with our regulated customers. When it comes to more direct involvement or participation by CSPs in an individual customers' BC/DR testing, it is important to highlight the following key points that make testing in a public cloud environment different to tests involving the parties currently in scope of Rule 1004:

   - Public cloud services are multi-tenant environments and the CSP must safeguard the CSP's other customers at all times;
   - All the CSP's customers retain significant control over the services (e.g. configuration, deployment); and
   - Traditional forms of BC/DR testing do not apply in the same way to cloud services as on-premise deployments.

   For example, with respect to the last bullet point above, A-B failover is a common form of 'recovery' testing in on-premise or private cloud environments. This can involve disconnecting primary production environments, or even an entire production data center (hot environment), to assess if services can be adequately transitioned (or "failover") to a secondary environment (warm/cold environment). If this practice were directly carried over

to the public cloud environment without being nuanced, it could lead to several perspectives that do not align to public cloud environments:

- An expectation that a public cloud provider should disconnect an entire production data center (typically referred to as a "region") to facilitate testing by a single customer. Undertaking this would necessarily disrupt the services for all other customers using that public cloud region.
- Cloud environments are built with service/product availability and reliability at the core - therefore, CSP production environments are replicated in every zone/region instance, meaning that failover testing is not a concept that carries over. Instead, capacity and capability are more relevant (i.e. can all services continue to run at production levels with a loss of capacity from a single zone or region being unavailable)
- SCI entities can test their alternate environments in a more 'traditional' failover manner, assuming their design/implementation is multi-homed and not single zoned, by simulating a region outage by configuring its own use of the services to route traffic away from a region (i.e. operating as if the region had gone offline) as is a common practice for their existing traditional on-premise infrastructure.

To reduce the risk of SCI entities directly requiring more traditional forms of testing to public cloud environments and inadvertently creating risk of other customers and stakeholders, we encourage the Commission address the nuance of BC/DR testing in public cloud environments and suggest the following adjustment to the proposed amendment:

"(b) designate members or participants and third-party providers pursuant to such standards and require participation by such designated members or participants and third-party providers in scheduled functional and performance testing of the operation of such plans, in the manner and frequency specified by the SCI entity, provided that such manner will take into account the nature of the services provided by the third-party provider and such frequency shall not be less than once every 12 months"

5. **Consistency Across Domestic (and International) Regulations.** Consistency regarding incident notification standards and requirements, as well as cybersecurity and system safeguards, across domestic and global regulators is critical in enhancing clarity, reducing costly and inefficient fragmentation, and ensuring the objective of identifying and mitigating actual cyber and technology risks. To this end, we applaud the FSB's recent work on incident notification[2] and the coordination across the U.S. banking regulators in promulgating recent

[2] Financial Stability Board (FSB), *Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting* (Oct. 17, 2022), available at https://www.fsb.org/wp-content/uploads/P171022.pdf.

rules. We further urge alignment with regulatory rule-making on incident reporting associated with the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022.[3] In order to advance consistency and regulatory convergence, we recommend the establishment and use of voluntary fora to help drive uniformity and for information sharing about threats/incidents that can be hosted jointly with other domestic and international regulators.

II. Conclusion

We appreciate the opportunity to provide our views on the Commission's Regulation SCI Proposal. We have a shared interest in making sure that the technology infrastructure of the U.S. securities market is protected. By pursuing convergence with respect to regulatory requirements consistent with domestic and global best practices, the Commission can most effectively and efficiently satisfy these objectives.

[3] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), available at https://www.congress.gov/bill/117th-congress/house-bill/2471/text.