U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

June 20, 2023

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Re: Solicitation for Public Comments on the Business Practices of Cloud Computing Providers (Docket ID FTC-2023-0028)

To Whom It May Concern:

The U.S. Chamber of Commerce appreciates the opportunity to comment on the cloud computing inquiry. The cloud computing sector is flush with competition from numerous companies both large and small, continues to see explosive investment and innovation, and takes great care to ensure the security of its customers' data.

Although we welcome the Federal Trade Commission's (FTC) inquiry, the Chamber does not see any new role for the Federal Trade Commission as it relates to data storage, data usage, data flows, or data security. The Chamber would also note that other U.S. agencies are better situated and already deeply engaged with the private sector to ensure security and resilience in relationship to national security considerations.

I. International Regulatory Environment and Challenges to Cloud Computing

The FTC released a blog post that accompanied the announcement of this inquiry noting that many other countries have undertaken similar evaluations to examine the cloud computing policy environment.[1] The blog post implied that the efforts in foreign jurisdictions were in part the impetus for the FTC query. The Chamber over the last several years has closely followed foreign jurisdictions as they seek to develop a policy framework for cloud computing and the Chamber has made multiple submissions to foreign cloud-type inquires. If there is one overarching lesson for the FTC to learn from cloud computing policy conversations around the world, it would be that many of those inquiries are grounded in or in part influenced by industrial policy objectives.

The United States is home to not only world leading cloud service providers, but an array of companies that provide services to the cloud customers. This has made the U.S. cloud services industry the envy of governments around the world causing those governments to

[1] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/inquiry-cloud-computing-business-practices-federal-trade-commission-seeking-public-comments

consider industrial policies to develop their own cloud service providers and limit the success of the foreign providers. There are also inquiries to better understand reliance and security, but even those often get intertwined with industrial policy motives that lead to flawed or misguided regulatory proposals.

This is part of a larger rise in digital protectionism and regulatory barriers that threatens to fragment the global internet, deny market access, and result in unfair or discriminatory treatment of U.S. companies to the advantage of domestic industry. Several jurisdictions, notably China, prohibit the use of U.S.-based cloud services through prescriptive requirements such as local data storage, local data access, local ownership, and restrictive cross-border data flows. For example, these policies include the proposed Korea Cloud Security Assurance Program which prohibits U.S. cloud service providers from competing on a level playing field in Korea's public sector market by requiring U.S. cloud service providers to build a separate Korea unique product architecture to participate in the government procurement process.

Most recently the EU has introduced a draft candidate scheme for cloud services cybersecurity certification (EUCS) that problematically includes sovereignty (corporate ownership) requirements for non-EU cloud service providers. According to the draft scheme, cloud service providers not headquartered in the EU would need to ensure immunity from non-EU law, localize data in the EU, and register a local presence in the EU.

Also in Europe, the European Union (EU) finalized the Digital Operational Resilience Act (DORA) in December 2022. DORA subjects financial institutions to set third-party risk management programs and reporting requirements related to cloud-related incidents. Undoubtably the EU's prescriptive rules will complicate financial institutions' adoption of global cloud services by creating conflicting, complex rules that may pose security risks.

These measures are unnecessarily restrictive and inconsistent with sound risk management practices and are contrary to the reality of the global architecture of cloud services. More like minded governments and industry trade associations have advocated for global, harmonized cloud requirements including the free movement of data, which are included in the United States – Singapore Joint Statement on Financial Services Data Connectivity.[2]

The Chamber has been active in bolstering supply chain resilience bilaterally and multilaterally with like-minded partners. We view cloud computing, along with semiconductors and digital infrastructure, as a key strategic area, fundamental to both the economic and national security of the U.S. As part of this effort, we consistently urge allies and partners with shared values to renew their commitment to working with the private sector to ensure that

[2] U.S. Treasury and Monetary Authority of Singapore, *United States – Singapore Joint Statement on Financial Services Data Connectivity* (Feb. 2020), https://home.treasury.gov/news/press-releases/sm899.

policy recommendations reject punitive approaches, new trade barriers, and one-size-fits all solutions.

II. Cloud Security, Risk Management, and Operational Resilience

The Chamber's member companies, including cloud service providers, critical infrastructure owners and operations, and small and midsize businesses, commit significant financial, technology, and human capital resources to cybersecurity, risk management, and operational resilience. We urge policymakers to adopt a risk-based approach and promote policies and frameworks that enhance trust, information sharing, and cooperation across public and private sectors. These important conversations are being led by other parts of the U.S. government.

General Observations on the Cybersecurity, Risk Management, and Operational Resilience Benefits of Cloud Computing.

In its 2023 U.S. National Cybersecurity Strategy released on March 2, the Biden Administration affirms the benefits of cloud computing in terms of cybersecurity and the resilience of U.S. critical infrastructure: "Cloud-based services enable better and more economical cybersecurity practices at scale, but they are also essential to operational resilience across many critical infrastructure sectors."[3] The pace of adoption of cloud services over the last decade has steadily increased across public and private sectors. The Chamber strongly supports cloud services and believes that properly configured, provisioned, and managed cloud architectures can be resilient and secure from various cyber and physical threats. Cloud adoption by critical infrastructure varies across industries and individual businesses. Early adopters of cloud services are frequently the most mature. In our experience, many companies use cloud services for non-critical business operations and have yet to migrate critical services or critical functions to cloud services. However, there are several virtues and unique challenges to cloud services, including:

- *Redundancy*. Most major cloud service providers leverage multiple data centers in regions across the globe. The architecture allows users to maintain synchronized data sets globally, resulting in little or no data loss if a client switches from one data center to another during disruptions. Of course, this is conditional on government policies that enable cross-border data flows. Cloud services providers and clients still rely on other lifeline sectors, e.g., broadband, internet communications, and electricity, for the uninterrupted distribution of services.

- *Scalability and speed to deploy assets*. One of the significant benefits of cloud services is the ability to rapidly develop, test, and deploy new applications and services, particularly in the case of artificial intelligence, vulnerability or zero-day event management and remediation, or workload capacity. Cloud service providers can

[3] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

quickly protect businesses against zero-day exploits by deploying patches in cloud environments. Cloud services, like any technology provider, have the potential for vulnerabilities to be discovered and exploited by malicious actors. In the case of the Log4j vulnerability discovered in December 2021, cloud service providers communicated with customers about the impact and remediation status of vulnerabilities and the steps that cloud customers could take to remediate systems.

- *Security*. The security capabilities of cloud services routinely meet or exceed on-premise capabilities, provided each cloud architecture is properly configured, provisioned, and managed. Key capabilities that distinguish cloud services from on-premises solutions include logging and encryption. Cloud services collect and retain logs and protect events through cryptographic methods to ensure their integrity. Cloud-based infrastructure offers various services to encrypt and decrypt data at rest or in transit with their associated logs.

  Although agencies' rules, guidance, and regulations for cloud service providers and critical infrastructure providers differ, the Chamber strongly urges policymakers to use and map to existing international standards and frameworks for a common cybersecurity baseline, including those developed and maintained by the International Organization for Standardization (ISO), the U.S. National Institute of Standards and Technology (NIST) (*e.g.*, NIST Cybersecurity Framework, NIST SP 500-291 Cloud Computing Standards Roadmap, or SP 500-332 Cloud Federation Reference Architecture), or sector-specific approaches, like the Cyber Risk Institute's "Cloud Profile."[4]

- *Shared Responsibility*. Security of cloud services, including public, private, or hybrid cloud, is a shared responsibility between the cloud service provider and the user. Often, whether in the contract or service level agreements, the technical, administrative, and security responsibilities are commonly detailed. The level of the cloud service providers' responsibilities for security and operational resilience generally increases along the continuum of infrastructure as a service to software as a service deployments.[5]

- *Third-party risk management* (TPRM). Increasingly, industry is developing or maturing approaches to third-party risk management, including through the procurement of cloud services. While each procurement and use are unique, typical TPRM processes may include: (1) risk-based due diligence of the use of cloud services to ensure that its use is consistent with the internal policies and compliance with appliable laws and regulations, (2) establish security and resilience controls against international standards (*e.g.*, ISO 27000 series), NIST (*e.g.*, SP 500-291, 500-332), or sector specific profiles (*iI.e.*,

[4] Cyber Risk Institute, Cloud Security Alliance, Bank Policy Institute, CRI Announces Completion of Cloud Profile Extension (Apr. 2022) https://cyberriskinstitute.org/cri-announces-completion-of-cloud-profile-extension

[5] GSA, Cloud Information Center, https://cic.gsa.gov/basics/cloud-security.

CRI Cloud Profile), (3) management and monitoring, which may including contract language or service level agreements for the evaluation of metrics (*e.g.*, uptime/downtime, event resolution) or periodic reporting on the evaluation of security (*e.g.*, service organization controls reviews, penetration testing, vulnerability assessment). Many aspects of a cloud users risk management program and their specific use of cloud services for business operations will inform their broader TPRM program.

Simply put, cloud computing is a critical tool for improving cybersecurity and defending critical infrastructure, American businesses, and consumers from malicious cyber activity. Cloud computing lowers the barriers to achieving state-of-the-art security for organizations of all sizes and budgets. It takes advantage of economies of scale to minimize the marginal cost of additional investments in security controls and expertise, and of implementing them at a global scale. This benefits customers, especially small- and mid-sized businesses, who may not have the resources or access to expertise to implement comparable cyber defenses on their own. In a recent blog post, Eric Goldstein, Executive Assistant Director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), urged "all [small and mid-sized businesses] with on-prem systems to migrate to secure cloud-based alternatives as soon as possible."[6]

U.S. Government Approach to Cloud Computing.

The US National Cybersecurity Strategy recognizes cloud computing as a critical enabler of U.S. government modernization and transition to secure architectures, with direct benefits for the U.S. public: "Replacing legacy systems with more secure technology, including through accelerating migration to cloud-based services, will elevate the cybersecurity posture across the Federal Government and, in turn, improve the security and resilience of the digital services it provides to the American people."[7]

The U.S. government has shifted its security policy and operations from focusing on perimeter-based defenses to a zero-trust model of security data, users, and services. In May 2021, President Biden issued Executive Order 14028 (EO 14028), Improving the Nations Critical Infrastructure, which articulates a vision for Zero Trust Architecture[8] and stipulates that the "Federal Government must … accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS)."[9]

---

[6] https://www.cisa.gov/news-events/news/accelerating-our-economy-through-better-security-helping-americas-small-businesses-address-cyber

[7] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[8] NIST, Zero Trust Architecture, by Rose, Scott, et al. (Aug. 2020), https://csrc.nist.gov/publications/detail/sp/800-207/final

[9] "Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity." 86 Fed Reg. 26633. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Following guidance from NIST, the Office of Management and Budget, and the Cybersecurity and Infrastructure Security Agency (CISA), U.S. federal agencies hope to accomplish this shift through security identity and access management for users and machines, ubiquitous encryption for data at rest and in transit, and accelerated adoption of cloud-based services.

To address urgent Solorigate response and recovery efforts, bolster cybersecurity defense, and accelerate cloud adoption by U.S. federal agencies, the U.S. Congress appropriated $1 billion in Technology Modernization funds in the American Rescue Plan. The TMF board prioritized cross-cutting agency projects and security enhancements, including $3.9 million for the U.S. Federal Trade Commission's Multi-Cloud Security Operations Center that will keep sensitive law enforcement, corporate competition filing, and American consumer data more secure and resilient to attack.[10] Replacing legacy IT systems with faster technology, including cloud services, will improve the security and resilience of the U.S. government's digital service.

In addition to the U.S. government's movement towards ZTA, the U.S. government promotes secure cloud adoption across the interagency through the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP promotes secure cloud adoption by standardizing security requirements for cloud services. Once authorized cloud products are placed in the FedRAMP marketplace, multiple agencies can leverage the security assessments conducted in the original assessment. Cloud service providers must also continuously monitor the security state of their products on the marketplace, conduct remediation, and report incidents.

In parallel with the drive for operational enhancements, the Biden Administration issued the President's National Cybersecurity Strategy earlier this year. It articulates the whole of society's approach to rebalancing the roles and responsibilities for securing cyberspace. Through the NCS and supporting national-level policies, the Biden Administration promotes cloud services as enablers of better and more economical cybersecurity and risk management at scale.

The NCS calls attention to critical workstreams for cloud services, harmonizing and streamlining new and existing regulations. The U.S. Chamber has long held government policies at home and abroad to enable effective cyber risk management when they leverage international standards. We look forward to working with the Office of the National Cyber Director, OMB, and CISA to pursue cross-border regulatory harmonization and reduce the risk of regulations that are in conflict, duplicative, or burdensome.

Growing cybersecurity concerns have caused U.S. and international regulators to increase cloud service provider requirements through new third-party risk management or

[10] Technology Modernization Fund, Multi-Cloud Security Operations Center (Accessed May 2023), https://tmf.cio.gov/projects/#multi-cloud-security-operations-center

supply chain security policies. **Table 1** highlights the breadth and depth of the certification, attestations, laws, regulations, standards, and frameworks global cloud service providers compliance teams must consider.

Table 1[11]

Global	U.S. Government	Industry	Regional
• CIS Benchmark • CIS STAR Attestation • CSA STAR Certification • CSA STAR SelfAssessment • CyberGRX • CyberVadis • ISO 20000-1 • ISO 22301 • ISO 27001 • ISO 27017 • ISO 27018 • ISO 27701 • ISO 9001 • SOC 1 • SOC 2 • SOC 3 • WCAG 2.0 (ISO 40500)	• JIS • CMMC • CNSSI 1253 • DFARS • DoD CC SRG • DoD IL2 • DoD IL4 • DoD IL5 • DoD IL6 • DoE 10 CFR Part 810 • EAR • FedRAMP • FISMA • FIPS 140-2 • ICD 503 • IRS 1075 • ITAR • JSIG • NIST 800-161 • NIST 800-171 • NIST 800-53 • NIST 800-63 • NIST CSF • Section 508 VPATs	**Automotive** • TISAX (Germany) **Education** • FERPA (US) **Energy** • NERC (US) **Financial Services** • 23 NYCRR 600 (US) • AFM + DNB (Netherlands) • AMF + ACPR (France) • APRA (Australia) • BaFin (Germany) • CFTC 1.31 (US) • CSSF (Luxembourg) • EBA (EU) • FCA + PRA (UK) • FFIEC (US) • FINMA (Switzerland) • FINTECH (Japan) • FINRA 4511 (US) • FISC (Japan) • FSA (Denmark) • GLBA (US) • KNF (Poland) • MAS + ABS (Singapore) • NBB + FSMA (Belgium) • OSFI (Canada) • OSPAR (Singapore) • PCI 3DS • PCI DSS Level 1 • RBI + IRDAI (India) • SEC 17a-4 (US) • SEC Regulation SCI (US) • Shared Assessments (US) • SOX (US) • TruSight **Healthcare and Life Sciences** • ASIP HDS (France) • GxP (FDA 21 CFR Part 11) • HIA (Canada, Alberta) • HIPAA (US) • HITRUST • MARS-E (US) • Medical Information Guidelines (Japan) • NEN 7510 (Netherlands) **Media and Entertainment** • CDSA • DPP (UK) • FACT (UK) • MPA **Telecommunications** • GSMA	**Americas** • Argentina PDPA • Brazil LGDP • Canada CCCS Assessment • Canada Privacy Laws • Canada Protected B • US CCPA **Asia Pacific** • Australia DTA HCF • Australia IRAP • Australia PDPA • China GB 18030:2005 • China DJCP (MLPS) • China ISO 20000 • China ISO 27001 • China ISO 27018 • China TRUCS/CCCPPF • China TCS • India MeitY • Japan APPI • Japan ISMAP • Japan CS Mark Gold • Japan My Number Act • Korea K-ISMS • Korea PIPA • Malaysia PDPA • New Zealand ISPS • New Zealand PDPA Philippines PDPA • Singapore MTCS Level 3 • Singapore PDPA • Taiwan PDPA • Thailand PDPA **Europe and Middle East** • EU CISPE Code • EU EN 301 549 • EU ENISA IAF • EU GDPR • EU Model Clauses • EU-US Privacy Shield Finland PiTuKri • Germany C5 • Germany IT–Grundschutz Workbook • Netherlands BIR 2012 Portugal GNS • Spain ENS High • Spain LOPD • Spain CCN SPSTIC • UK NCSC Cloud Security Principles • UK Cyber Essentials Plus • UK G-Cloud • UK PASF **Middle East and Africa** • South Africa POPI • Qatar NIA • UAE DESC

The Chamber urges the FTC to enhance its domestic collaboration with sector risk management agencies, the National Institute of Standards and Technology, the Cybersecurity and Infrastructure Security Agency, the Office of Management and Budget, and the Office of the National Cyber Director, especially on existing workstreams related to the criticality of cloud service (e.g., updating Presidential Policy Directive 21), the harmonization of the cyber incident reporting via the Cyber Incident Reporting Council at the Department of Homeland Security, and the harmonization of a common cybersecurity baseline.

III. Cloud & Data Protection

While cloud storage is widely viewed as among the safest options for storing data, data breaches can and do occur, as they occur in on-premises storage solutions. Similarly to breaches that arise from other modes of data storage, the Federal Trade Commission is well positioned to enforce the law. Cloud computing and storage does not present significant new consideration to the FTC for how to respond to cloud related data breaches. In fact, the FTC cited, as part of its announcement of its cloud inquiry, actions it took against Drizly[11] and Chegg[12] as examples of the agency already capable of enforcing the law in the context of the cloud.

The cloud industry takes data breaches seriously. The misconfiguration of cloud services by clients is the cause of most security incidents. Thus, a significant factor contributing to cybersecurity incidents is the need for more skilled cloud security and architecture experts relative to the demand for cloud services. General information technology (IT) and cybersecurity skills only fully translate to cloud expertise with additional training or upskilling, but such training is readily available. Similarly, skills associated with the deployment and security of one cloud service provider are only sometimes interoperable with the deployment and security of another cloud service provider. Cloud users are investing in reskilling general IT workers for cloud migration and risk management. Cloud service providers are increasing their educational events and deploying more tools (*e.g.,* automated tools and dashboards to recognize misconfigurations).

[11] FTC Finalizes Order with Online Alcohol Marketplace for Security Failures that Exposed Personal Data of 2.5 million People | Federal Trade Commission

[12] https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-finalizes-order-ed-tech-provider-chegg-lax-security-exposed-student-data

IV. The Cloud Increases Competition

Cloud computing is competitive. Companies, large and small, foreign, and domestic, are vigorously competing to serve customers, and they are competing against on-premises providers of IT goods and services. Many companies offer services in the full stack while others specialize in different segments. Importantly, looking solely at the group of hyperscale providers that each offer their own full cloud stack does not fully capture the competition and innovation at all layers of the cloud stack.

The FTC's request for information asked questions on the three main service models described in the National Institute of Standards and Technologies' definition of cloud computer, Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). SaaS represented the largest layer by revenue, or approximately $178 billion according to the International Data Corporation in 2021, followed by IaaS ($115 billion) and PaaS ($111 billion).[13] SaaS applications are the most common and include many non-critical business functions like corporate employee operations, human recourses software, accounting, email, customer relationship management systems, document collaboration, video conferencing, or high-traffic customer-facing applications.

These companies compete across a range of issues and offer customers a range of contractual options. In terms of price, cloud providers use various pricing models, such as pay-as-you-go, subscription pricing, tiered pricing, reserved instances, and spot instances. As with other products and services, providers often offer discounts to customers who commit to long-term contracts or use more services. As a result, customers can pick and choose from a variety of contractual options to tailor the quantity, duration, and level of their cloud spending to their needs. In negotiating contracts, customers often seek the assistance of experienced third parties, such as consultants or attorneys, who can help to identify potential opportunities.

Beyond price and volume, cloud providers also compete on other dimensions, including service and security. Cloud providers invest heavily in security measures to protect their customers' data, such as multi-factor authentication, encryption, and network security. Similarly, providers offer different levels of support, from self-service to constant support from dedicated technical teams. Service levels also can depend on whether the company operates at one layer or multiple layers of the cloud computing stack, and many companies provide various training and certification programs to help customers develop the skills they need to use their products effectively.

As a result of this competition, and strong market demand, investment and innovation levels have taken off.[14] According to one industry report, in 2020, cloud providers spent around

[13] International Data Corporation, Worldwide Semiannual Public Cloud Services Tracker H2-2021.

[14] In the Solicitation, the FTC asks whether investment has been "sufficient." Respectfully, it is not the province of the FTC to determine whether businesses should invest more or less in a particular technology versus other technologies or other things entirely. Nevertheless, a cursory review of the facts reveals that cloud investment remains very high by almost any metric.

$129 billion on capital expenditures, a significant portion of which was invested in R&D. According to Gartner, a technological research and consulting firm, public cloud services spending grew from $220 billion in 2016[15] to $411 billion in 2021, and it is estimated to reach nearly $600 billion in 2023.[16] On an ongoing basis, cloud providers are seeking to improve the performance, scalability, security, and reliability of their cloud computing services and to develop new features and services that enable customers to leverage emerging technologies, such as artificial intelligence, machine learning, and the Internet of Things. Cloud providers also collaborate with academic institutions and research organizations to advance innovation, such as by sponsoring research projects, providing access to their cloud infrastructures for research purposes, or working with researchers to develop new technologies and services.

In short, competition in the cloud is thriving. As the FTC studies cloud services, it should keep in mind that premature and excessive regulations could harm consumers. For instance, new regulations invariably would increase compliance costs for cloud providers, which could reduce their willingness or ability to innovate and compete on price. Similarly, regulations could create barriers to entry for new cloud providers by increasing the cost of compliance for data protection. Often, premature and excessive regulations can lead to unintended consequences, such as favoring established players over new entrants or favoring certain business models over others. Such a result could stifle innovation and reduce competition. This caution against excessive regulation includes the FTC's oversight over mergers. To foster additional competition in cloud computing, the FTC should recognize that highly capitalized companies with strong reputations or large numbers of users in adjacent markets might be best positioned to reposition into the cloud market, where scale is important. Thus, the agency should not prevent companies from acquiring the resources to be successful players in the cloud market simply because they have a strong presence in other markets.[17] Finally, regarding any attempt to regulate data portability or dictate the transferability of software licenses, such action would be beyond the scope of the Federal Trade Commission's authority.

V. Conclusion

The Chamber appreciates the opportunity to submit these comments. The United States is a leading provider of cloud infrastructure and services, and a foreign regulator's motives should be carefully evaluated before being duplicated. The FTC should take note that several other agencies of the U.S. government are deeply engaged with the private sector on critical issues of resiliency and security. Further, data breaches from the cloud are no different than

[15] Gartner, Gartner Forecasts Worldwide Public Cloud Services Revenue to Reach $260 Billion in 2017 (Oct. 2017).
[16] Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023 (Apr. 2022), https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecastsworldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022.
[17] See, e.g., How the New Anti-Merger Policy May Be the New Antitrust Paradox, Maureen K. Ohlhausen & Taylor Owings (Nov. 9, 2022) Competition Policy Int'l, https://www.competitionpolicyinternational.com/how-the-new-anti-merger-policy-may-be-the-new-antitrust-paradox/

data breaches that arise from other forms of data storge, the FTC is already capable of addressing such instances. Finally, cloud computing by any measure is a competitive business.

Sincerely,

Sean Heather
Senior Vice president
International Regulatory Affairs and Antitrust
U.S. Chamber of Commerce