June 21, 2023

VIA ELECTRONIC SUBMISSION

April J. Tabor
Secretary of the Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580

Re: Solicitation for Public Comments on the Business Practices of Cloud Computing Providers

Dear Ms. Tabor:

The Alliance for Digital Innovation (ADI) appreciates the opportunity to submit this letter to the Federal Trade Commission (the FTC or the Commission) in response to the Commission's Solicitation for Public Comments on the Business Practices of Cloud Computing Providers, issued on March 22, 2023 (hereinafter, the RFI). ADI submits this letter on behalf of our members, which include cloud service providers (IaaS, PaaS, and SaaS), cloud service integrators, cybersecurity companies, and end-user cloud-based technology companies that service public sector entities at the United States federal and state levels. Our members represent a cross-section of technology and service providers, all of which are dedicated to meeting and exceeding the needs of our public sector customers. To this point, ADI believes that any practices that artificially limit the choices that our public sector institutions have when selecting the optimal solution for their missions can cripple the delivery of critical services to our communities.

We submit this letter to answer several questions posed by the RFI. In particular, we provide examples and use cases of public sector institutions along with recommendations for building customer-led pathways to robust IT modernization and cloud migration. Further, we urge the Commission to take the experiences in the public sector into consideration when deliberating future actions across commercial sectors. There is much that can be learned from the last fifteen years of public sector cloud adoption and growth – from the benefits of secure compliance regimes to the harms of certain software licensing practices. As the federal government looks to use its purchasing power to drive changes and develop best practices, the FTC can use those experiences to better understand the dynamics and impact of the cloud services.

Commenting Organization

The Alliance for Digital Innovation (ADI) is a non-profit coalition of innovative, commercial companies whose mission is to bring IT modernization and emerging technologies to government. ADI member companies include a wide range of cloud service providers (including IaaS, PaaS, and SaaS providers), small and midsize innovative integration companies, and other innovative, cutting-edge technology companies, all supporting the public sector. Our members provide key critical technologies at all levels of the government's technology stack, including cloud infrastructure, digital identity, human resources software, quantum computing, digital services, and a range of sophisticated cybersecurity tools and services critical to public sector missions. Our goal is to break down institutional, systemic, and legal barriers to bring the technological advancements in commercial innovation to the public sector and help build a modern, 21st century digital government.

Overview and Background

Public sector organizations have seen a steady increase in the use of cloud technology over the last fifteen years, with accelerated growth during the pandemic.[1] According to Deltek's federal market analysis, the federal government spent $12.3 billion on cloud products and services in FY22 alone.[2] This significant increase in cloud consumption by the public sector is only the beginning of continued investment and growth in infrastructure (IaaS), platform (PaaS), and software as a service (SaaS). At the state level in 2020, the Digital Counties Survey reported that only 12 percent of respondents had moved more than half their systems to cloud services.[3] Before discussing the particular challenges facing public sector migration to cloud services, we wanted to provide some background on the policy environment that has driven cloud adoption and that continues to shape its acquisition today.

In February 2011, Vivek Kundra, then the U.S. Federal Chief Information Officer, released the first Federal Cloud Computing Strategy,[4] calling for a "cloud first" approach to federal IT modernization efforts. This strategy jump-started several efforts across the federal government, many of which shape the federal and state public sector today. Some of the resulting standards, policies, and programs include:

---

[1] https://www2.deloitte.com/us/en/insights/industry/public-sector/public-sector-cloud-adoption.html

[2] https://iq.govwin.com/neo/marketAnalysis/view/Federal-Cloud-Spending-FY-2020-2022/7171?researchTypeId=1&researchMarket=PFMAP#:~:text=Total%20Cloud%20Spending,on%20cloud%20goods%20and%20services.

[3] https://www.govtech.com/cloud-different/the-state-of-cloud-in-state-and-local-governments

[4] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

- NIST SP 800-145,[5] which defines cloud computing. This is one of several documents produced by NIST in 2011 that helps standardize the vernacular.

- OMB's Federal Risk and Authorization Management Program (FedRAMP) Memo, titled *Security Authorizations of Cloud Computing Systems in the Federal Government.*[6] This memo initiated a program that developed security practices and policies that cloud companies must follow to secure their environments.

- OMB Circular A-130,[7] *Managing Information as a Strategic Resource*, which identifies cloud computing as part of a broader set of information technology.

In addition to the administrative efforts, Congress also passed or updated several laws to enable the government to develop a cohesive approach to cloud adoption in the federal government. Examples of those laws include:

- The Federal Information Technology Acquisition Reform Act (FITARA), which empowered agency CIOs while directing agencies to modernize their infrastructure and information technology architectures.

- The Federal Information Security Modernization Act (FISMA), which provides authorities to various administrative offices to oversee the risk management of federal government cybersecurity.

- The Modernizing Government Technology (MGT) Act, which authorized the use of a centralized technology modernization fund (TMF) as well as providing each agency with its own working capital fund to drive investments in modern cloud services.

- The FedRAMP Authorization Act, which authorized and expanded the FedRAMP program to enable a unified approach to the risk management of the adoption of cloud services.

These laws, coupled with the administrative policies and standards, demonstrate a move to guide federal agencies in their adoption of cloud products and services.

Cloud Acquisition in the Federal Government

Over the past fifteen years, there have been several attempts to direct the secure acquisition of cloud products and services. From government-wide acquisition contracts (GWAC) to agency-specific indefinite delivery, indefinite quantity (IDIQ) contracts, the federal government's approach to acquiring cloud services has evolved over the last

[5] https://csrc.nist.gov/publications/detail/sp/800-145/final

[6] https://federalnewsnetwork.com/wp-content/uploads/pdfs/fedrampmemo.pdf

[7] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

decade and a half. Additionally, as discussed above, the FedRAMP program has also grown and changed over the years to fit the varying needs of departments and agencies. Below are some important acquisition or security compliance milestones that have occurred over the last fifteen years.

GWACs and IDIQs and Consumption Based Pricing in the Government

To facilitate the procurement of cloud computing goods and services, the federal government has turned to use of GWACs and IDIQs as a "best practice" in acquisition methodologies.[8] These contracts streamline the procurement process for acquiring a wide range of goods and services, and are typically awarded to a select group of qualified vendors after a competitive bidding process. GWACs provide government agencies with an efficient and cost-effective means to acquire technology products and services, including cloud computing solutions.[9]

While GWACs and IDIQs offer numerous benefits, one challenge to the implementation of cloud-based technologies by government agencies is the absence of a true consumption-based billing methodology that is available to the federal government.

In commercial practice, most cloud-based goods and services are billed in arrears for those resources that are *consumed.* In other words, most cloud providers allow customers to consume their products and services first, and then make payment in arrears. This attribute of cloud services provides an enormous benefit to cloud customers because they pay *only for those cloud resources that they consume.* This allows commercial cloud customers to avoid having to park contingency funds or otherwise buy "stand by" capacity in advance, freeing up customer financial resources to more productive investments elsewhere.

Unfortunately, the federal government cannot avail itself of this significant commercial benefit due to the nature of appropriations law constraints. For instance, the Anti-Deficiency Act[10] requires agencies to obligate specific funds *in advance,* before they can buy or consume any product or service. Further, 31 USC § 3324 prohibits advance payments, which makes purchasing reserved instances of cloud computing capacity challenging. As a result, agencies buying cloud services must project the totality of their cloud computing consumption ahead of time, so that procurement teams can obligate funding in advance and hope that their actual needs over the life of the contract do not exceed that budgeted/obligated amount.

[8] A description of the most active GWACS as well as commentary on their attributes is available from GSA at Governmentwide Acquisition Contracts (GWACs) | GSA

[9] Governmentwide Acquisition Contracts (GWACs) | GSA

[10] The Anti-Deficiency Act is 31 U.S. Code Section 1341, available at 31 U.S. Code § 1341 - Limitations on expending and obligating amounts | U.S. Code | US Law | LII / Legal Information Institute (cornell.edu)

The General Services Administration (GSA) has attempted to create an administrative solution to this problem by allowing consumption-based payments that are founded on smaller *advance* obligated appropriated dollars under the GSA Schedules program.[11] However, adoption of the guidelines outlined in GSA's 2020 memo has been limited, as the guidance does not solve the fundamental incompatibility between needing to pre-obligate federal funding on a contract and consumption-based payment in arrears for cloud service usage.

Department of Defense Cloud Acquisition Approach

The United States Department of Defense (DoD) states in its strategies and public statements that it wants to pursue a strategy of Joint All-Domain Command and Control (JADC2). To implement this joint approach, the DoD Chief Information Officer pursued an approach to enterprise cloud adoption that would allow for the sharing of data across organizational boundaries: the Joint Warfighting Cloud Contract (JWCC) vehicle for cloud procurement.[12] This procurement vehicle was awarded in 2022 to four cloud providers and allows for the various organizations within the DoD to contract directly with the various providers for cloud services. Currently, the DoD is competing individual task orders to the companies that won individual JWCC IDIQ contracts.[13] This allows for robust competition among the cloud service providers that won spots on JWCC, as well as their partner networks.

FedRAMP and the DOD Cloud Security Requirements Guide

Across the federal and state governments, there is a number of programs aimed to help public sector departments and agencies managing risk and security compliance requirements when adopting cloud technology. The cornerstone of those programs is the Federal Risk and Authorization Management Program (FedRAMP), which began in 2011. This program was created to help federal government agencies manage their internal information technology risk and to guide agencies as they move workloads from government-owned and -operated data centers into data centers managed by cloud providers. One of the most significant contributions of FedRAMP is the creation of a centralized repository of security controls and best practices known as the FedRAMP Security Assessment Framework. This framework establishes a baseline for security controls, ensuring consistent security requirements across federal agencies. The frameworks outlines how cloud service providers (CSPs) should implement National

[11] Acquisition Letter MV-20-01 Date MEMORANDUM FOR THE GSA ACQUISITION WORKFORCE FROM: JEFFREY A. KOSES SENIOR PROCUREMENT EXECUTIVE OFFICE OF ACQUISITION POLICY (MV) SUBJECT: Procurement of Cloud Computing on a Consumption Basis; available at https://federalnewsnetwork.com/wp-content/uploads/2020/01/MV-20-01-Consumption-Based-Cloud-Computing-External-Distribution-1.17.2020-1.pdf.

[12] https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/

[13] https://www.c4isrnet.com/smr/cloud/2023/05/04/first-secret-task-orders-received-for-pentagons-9b-cloud-contract/

Institute of Standards and Technology (NIST) security controls in their solutions. By doing so, FedRAMP enables CSPs to demonstrate compliance with these requirements, reducing duplication of efforts and saving time and resources across government.

The impact of FedRAMP on cloud services is substantial. It has instilled confidence in federal agencies to adopt cloud services by providing a rigorous security assessment process. Cloud providers that achieve FedRAMP compliance gain a competitive edge as they are recognized as having met the stringent security standards set by the federal government.

Following the development and release of the guidance and "security baselines"[14] from the FedRAMP program management office (PMO), the DoD developed its own cloud computing security guidance (DoD Cloud SRG or CC SRG[15]), which built onto the FedRAMP bases to address the unique security concerns of the DoD, including protecting classified information, ensuring mission continuity, and maintaining compliance with federal regulations. Importantly, the DoD Cloud SRG offers reciprocity with the FedRAMP baselines that map directly to specific NIST controls at the various "impact levels" identified in the document.

The DoD's adoption of cloud computing has been instrumental in driving innovation and efficiency within the defense sector, and the DoD Cloud Security SRG plays a vital role in addressing the unique security requirements of the DoD. By establishing a standardized set of security controls and guidelines, the SRG and the superior security cloud providers offer ensure that DoD missions and sensitive data are adequately protected in the cloud.

CSPs that meet the rigorous security requirements of the SRG are positioned as trusted partners of the DoD. This provides a competitive advantage and opens lucrative opportunities within the defense sector. The SRG also fosters collaboration between CSPs and the DoD, leading to the development of innovative solutions tailored to meet the specific security needs of the defense community.

The above security requirements, while streamlined and reciprocal, are often onerous and difficult to achieve for many cloud companies that do not initially build commercial tools with those specific NIST security controls in mind.[16] They often require

---

[14] https://www.fedramp.gov/baselines/

[15] The **DoD Cloud Computing Security Requirements Guide** (SRG) is a document that provides a standardized process for cloud service providers (CSPs) to gain a DoD provisional authorization (PA) to host DoD missions. It defines the baseline security requirements for different levels of impact and sensitivity of the data and systems hosted in the cloud. It is developed and maintained by the Defense Information Systems Agency (DISA), an agency of the U.S. Department of Defense (DoD). It supersedes and rescinds the previous DoD Cloud Security Model (CSM) and maps to the DoD Risk Management Framework (RMF). SRG Government Services is a different entity that is a DoD and Federal Contractor that specializes in staff augmentation and surge recruiting. The terms of the SRG are available at Jan_26_Control_Systems_SRG.pdf (cyber.mil)

[16] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

significant investments in product architecture and design that are not required – and often not optimal – for a broader commercial approach and can be more resource-intensive for small and midsize cloud service providers. This can unintentionally restrict public sector departments and agencies from accessing the latest commercial technology available. While flexibilities in risk-management approaches create some opportunities, most of the public sector cloud consumers default to a higher level of security without considering the access implications. Part of the reason for the development of the FedRAMP program was to provide an approach that would mitigate perceived security concerns.[17] However, requirements that stem from unfounded security concerns can lead to slower cloud adoption, which stifles innovation and competition for large and small CSPs alike.

As the FTC considers whether cloud companies are adequately addressing security concerns, it should consider the significant scope of security compliance regimes like FedRAMP and the DoD Cloud SRG. Further, the FTC should learn from the development of these security requirements and the reciprocity granted by the different government organizations. These requirements – while different – are based on the same NIST security controls and therefore allow for acknowledgment and reciprocity across compliance functions. Finally, the FTC should recognize the burden associated with meeting these various thresholds of security, and that additional regulations may unintentionally limit competition.

Current Challenges in IT Modernization

As noted above, the public sector has been investing in cloud services for over a decade and a half. It continues to experience many of the same challenges that other industry sectors are facing in their efforts to migrate to more cloud-based environments. Below are some examples of competition issues that government buyers are wrestling with as they invest in cloud services.

Restrictive Software Licensing Practices

In January 2023, the National Aeronautics and Space Administration (NASA) Office of the Inspector General (OIG) released a report estimating that NASA could have saved $35 million through use of better software asset-management practices. Of that $35 million, the OIG claimed that $15 million of the savings could have been saved by limiting the number of unused licenses.[18] This report highlights two historical scenarios:

> ***Vendor lock-in.*** *A situation in which a customer using a product or service cannot easily transition to a competitor's product or service. NASA purchased large amounts of [vendor] products to support Space Shuttle processing and*

[17] https://www.computerworld.com/article/2550034/cloud-fears-are-overblown-says-u-s-cio.html

[18] https://www.oversight.gov/sites/default/files/oig-reports/NASA/IG-23-008.pdf

> *other mission operations during that timeframe containing licensing terms that made transitioning to a competitor difficult due to proprietary technologies.*
>
> ***Status-quo renewal.*** *NASA has been unwilling to risk a license audit by [a particular vendor] because of the lack of solid, centralized visibility into deployment and use of the software. OCIO officials explained that they "knew better than to try our luck with an audit." Simply put, merely the potential threat of being audited by the vendor encouraged overbuying when the accuracy of Agency Software Asset Management was suspect.*

The report goes on to state that the Office of the Chief Information Officer (OCIO) has committed to fully addressing the overspending addressed in the above anecdotes. The OCIO also noted that to prepare for discussions around contract renewal, the office is meeting internally to determine "how and why" the licenses from that vendor became so complex and difficult to manage.

Tying Services to Promote Single Vendor Adoption

In addition to anti-competitive software licensing practices, some companies leverage their market position to tie use of their popular software products to other products and services.[19] ADI does not believe that bundling services is inherently anti-competitive. However, when a company ties its products that have significant market share with its other products and services, it creates a bias to that company's own solution. Major areas of enterprise cloud services are impacted by practices outlined above, including file hosting and collaboration, cybersecurity, identity access and credential management, and video conferencing. In fact, Congress has started to investigate the potential harms of some of these anti-competitive practices.[20]

In a letter[21] to the Secretary of Defense from February 2023, Rep. Dutch Ruppersberger – a senior member of the Defense Appropriations Subcommittee – expressed the following concerns:

> I am concerned the Department may default to the "path of least resistance" in the name of achieving Zero Trust Strategy at the cost of competition from a diverse set of cybersecurity vendors and ultimately putting mission at risk with inferior solutions. Procurement vehicles that only allow for large technology companies with significant market power . . . to bundle operating systems, applications, and cybersecurity into large enterprise-wide agreements limit competition and fail to appropriately value the cybersecurity merits of the proposed solutions.

[19] https://www.kieferconsulting.com/Documents/G5_eBook.pdf

[20] https://www.newsweek.com/pentagons-microsoft-monopoly-raises-cybersecurity-concerns-congress-dod-defense-1804884

[21] https://d.newsweek.com/en/file/466289/rupperberger-cybersecurity-letter.pdf

The letter also points out the need for fair and open competition for DoD cybersecurity solutions that are based on technical merits. ADI recommends that public sector agencies create an acquisition culture that ensures prioritized solutions that are best-in-breed as opposed to those that are tied to other solutions and are technically acceptable.

Need for Competition in Cybersecurity

There are many cloud service providers that offer a variety of services – including security services. In the cybersecurity space, in particular, the public sector has a responsibility to foster competition for the solutions that have the best technical merits. More specifically, the public sector should ensure it has the ability to build a robust system of checks and balances into its security environment. ADI believes in multilayer cyber defenses and supports acquisition environments that allow customers to choose a separate provider to assess and report on vulnerabilities in a cloud computing environment rather than the provider responsible for that environment. More specifically, public sector institutions should create a procurement environment that encourages competition among cybersecurity solution providers that provide best-in-breed services and enable agencies to detect and mitigate threats across their networks and at their endpoints, focus on finding vulnerabilities, enable agencies to prioritize their own patching and vulnerability management programs, effectively manage their identities across environments, and provide the best threat intelligence in the marketplace.

Representative Ruppersberger notes this need in his February 2023 letter, saying,

> Given the many components needed for a comprehensive cybersecurity solution that meets DoD's Zero Trust Strategy, such as Endpoint Detection and Response, Identity and Access Management, Vulnerability Management, and Security Information and Event Management, it is critical that DoD pursue a fair and open competition that ensures procurements for cybersecurity solutions are based on technical merits and are not limited to a single one-size-fits-all enterprise solution.[22]

While the congressman is focused on the Department of Defense, this need for robust competition and customer choice in setting up a secure environment is paramount for all public sector organizations. Given the important missions and sensitive information that the government maintains, public sector entities have a responsibility to build as secure an environment as possible as they modernize their information technology solutions.

Conclusion

The public sector has been acquiring cloud products and services for many years. The federal government, in particular, built policies and processes to manage risk,

[22] https://d.newsweek.com/en/file/466289/rupperberger-cybersecurity-letter.pdf

facilitate procurements, and measure implementation. While these programs and practices have helped facilitate an initial move to more modern environments, there are still many governance and programmatic changes that must be made. That said, the FTC can learn from the experience of the public sector. Some key points for consideration are as follows:

- The public sector must continue to streamline its compliance requirements and foster reciprocity across its compliance programs. Reciprocity and harmonization of requirements can elevate security while removing compliance burdens that can act as deterrents for both large and small innovate cloud companies;

- The FTC must foster an open and competitive environment that allows for nimble, innovative businesses – including small, midsize, and large cloud companies – to compete fairly. This means identifying instances of tying products together across an enterprise IT environment through use of market power; and

- The public sector must build better organizational understanding of its software environment to help defend against restrictive software licensing practices that can lead to vendor lock-in or perpetuate purchasing of unused licenses. The FTC can help commercial institutions understand the risks associated with predatory software licensing practices and identify best practices for asset management and licensing agreements.

The Alliance for Digital Innovation appreciates the ability to submit these comments for the Commission's consideration. As the FTC continues its research into cloud competition and security, ADI stands ready to provide any additional insight or feedback that the Commission's needs. Thank you again for the opportunity to engage on such an important topic.

Sincerely,

The Alliance for Digital Innovation