July 21, 2026

Association for Competitive Technology

Ministry of Digital Development and Information
140 Hill Street, #01-01A
Old Hill Street Police Station
Singapore 179369

Infocomm Media Development Authority
10 Pasir Panjang Road, #03-01
Mapletree Business City
Singapore 117438

RE: Comments of the Association for Competitive Technology on the Draft Digital Infrastructure Bill

The Association for Competitive Technology (ACT) appreciates the opportunity to submit views to the Ministry of Digital Development and Information (MDDI) and the Infocomm Media Development Authority (IMDA) on the draft Digital Infrastructure Bill (Bill). ACT represents the small business and startup technology developer community both in Singapore and around the world that creates the software and connected devices driving internet of things (IoT) use cases across consumer and enterprise contexts and rely on a vibrant digital infrastructure. Today, the value of the ecosystem ACT represents is approximately S$2.3 trillion and is responsible for millions of jobs worldwide and serves as a key driver of the S$10.3 trillion IoT revolution.[1]

ACT members build and deploy products and services across communications, health, education, retail, finance, mobility, and industrial applications. As leading consumers, developers, and adapters of artificial intelligence (AI) and other cloud-enabled tools, they have a major stake in the availability of robust, reliable, scalable, and affordable digital infrastructure.

ACT commends MDDI and IMDA for seeking to uplift the security and resilience of major cloud computing and data centre services as well as the environmental sustainability of data centre operations. Digital infrastructure services are a foundational part of Singapore's growing digital economy, enabling digital services used by businesses and consumers across the economy. The Bill's focus on major providers, and its initial exclusion of Software-as-a-Service (SaaS), reflect an appropriately targeted starting point.[2]

[1] Association for Competitive Technology, Fast Facts, https://actonline.org/wp-content/uploads/Fast-FactS_Website.pdf.
[2] Ministry of Digital Development and Information and Infocomm Media Development Authority, Public Consultation on Digital Infrastructure Bill (1 July 2026), https://www.mddi.gov.sg/newsroom/public-consultation-on-digital-infrastructure-bill/.

1401 K Street, NW, Suite 501
Washington, D.C. 20005

+1 (202) 331 - 2130 www.ACTonline.org /US-ACT @ACTonline

Much of the conversation around data centres and cloud infrastructure focuses on the ambitions of the world's largest technology companies. This focus, while understandable, overlooks a fundamental truth: small businesses are the primary consumers of the AI tools and cloud services that data centre infrastructure enables. Cloud computing services have given small businesses and startups greater flexibility, scalability, accessibility, and cost savings, while also enabling innovation and accelerating time to market for new services and applications. Cloud services provide small businesses with access to cost-effective solutions and on-demand scalable infrastructure support that allow them to focus on their core operations and their customers' needs. Research has likewise found that cloud computing can help smaller and newer firms compete.[3]

ACT members are not only users of this infrastructure. They also build much of the digital layer that a modern data centre depends on, including the infrastructure-management, monitoring, observability, environmental-sensing, security, and energy-optimisation software and connected devices that help these facilities run securely, resiliently, and efficiently, which are precisely the outcomes the Bill seeks. As IMDA develops codes of practice and implementing instruments, it should take care that Singapore's policy framework does not inadvertently foreclose this small digital-supplier tier and should keep opportunities open to the small software and connected-device firms that supply these tools.

ACT therefore supports the Bill's core objectives while urging a clear, risk-based, internationally interoperable, and proportionate implementation. The final framework should preserve a predictable scope; coordinate with the Cybersecurity Act and internationally recognised standards; allocate obligations according to operational control and the ability to mitigate risk; protect confidential and security-sensitive information; and account for downstream effects on small-business access.

Preserve a Narrow, Risk-Based, and Predictable Scope

ACT welcomes the government's decision to focus the regime on major foundational digital infrastructure services rather than regulating every provider or customer in the digital ecosystem. In introducing the foundational digital infrastructure provisions under the Cybersecurity Act, the Government explained that the framework would cover major providers serving a large number of businesses or organisations and that smaller players, which are more sensitive to regulatory costs, would not be regulated. That targeted and calibrated approach should remain central to the Digital Infrastructure Bill.[4]

---

[3] Nicholas Bloom and Nicola Pierri, Research: Cloud Computing Is Helping Smaller, Newer Firms Compete, Harvard Business Review (31 Aug. 2018), https://hbr.org/2018/08/research-cloud-computing-is-helping-smaller-newer-firms-compete. *See also* ACT, Follow-up Views on "Powering America's AI Future: Assessing Policy Options to Increase Data Center Infrastructure" (13 Mar. 2026), https://actonline.org/wp-content/uploads/Letter-from-The-App-Association-March-13-2026-1.pdf.

[4] Cyber Security Agency of Singapore, Opening Speech for Second Reading of Cybersecurity (Amendment) Bill by Senior Minister of State Janil Puthucheary (7 May 2024), https://www.csa.gov.sg/news-

Clarify coverage and preserve the SaaS exclusion

For small and medium-sized enterprises (SMEs), predictability depends on whether the relevant legal standards, evidentiary expectations, and procedural pathways are sufficiently clear in practice. Businesses benefit where guidance and process make clear the kinds of evidence likely to be considered relevant, the criteria likely to be applied, and the manner in which affected stakeholders may engage. Smaller firms in particular benefit from clarity that allows them to allocate limited resources effectively. While the Bill specifies a threshold for data centre facility service at a critical IT load of 10 MW or more, a cloud computing service that has generated S$100 million or more in revenue from users in Singapore on average over the three preceding years within the Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) categories but not SaaS, and a 3 MW critical IT load for the data centre licence, IMDA should clarify what constitutes a 'large number' of businesses or organisations and whether meeting a Schedule threshold is by itself sufficient for coverage or whether a provider below a threshold could still be captured through the 'large number' limb of the statutory definition; how revenue 'from users in Singapore' will be attributed, including how the definition of a 'user in Singapore' applies to registered or incorporated business entities and to ordinarily resident individuals, and how the three-year average is calculated for new entrants and partial financial years; the treatment of affiliated entities, resellers, channel partners, bundled services, free credits, acquisitions, partial financial years, and multi-region contracts; and the classification of hybrid services that include elements of IaaS, PaaS, managed services, serverless computing, developer tooling, and SaaS. Providers should be able to seek an advance coverage determination, and the framework should provide a clear process for removing a service from the regime when it no longer satisfies the statutory criteria.

ACT strongly supports preserving the initial exclusion of SaaS. The final framework should also make clear that a small application developer, connected-device company, cloud customer, reseller, or managed-service provider does not become a major foundational digital infrastructure service provider merely because it uses third-party cloud infrastructure, offers an application programming interface (API), bundles cloud functionality, or manages a customer workload without controlling the underlying infrastructure.

Avoid unnecessary barriers for cross-border providers

The Bill requires applicants to maintain a permanent place of business or registered office in Singapore and at least one locally connected officer. However, because the Bill's sections 8(8) and 10(4) would already permit a provider located outside Singapore to appoint a person in Singapore to accept service of notices and documents, the service-of-process objective could be met without a significant local-presence criteria. IMDA should therefore permit functionally equivalent arrangements for the place-of-business and local-officer criteria, including by prescribing an appropriate class of persons under sections 9(3)(c)(iii) and 23(6)(c)(iii), so that accountability is preserved without foreclosing qualifying cross-border participation. The licensing framework should not unnecessarily discourage a qualifying cross-border provider from serving Singapore where the provider can satisfy all substantive security, resilience, reporting, and enforcement

---

events/speeches/opening-speech-for-second-reading-of-cybersecurity-%28amendment%29-bill-by-sms-janil-puthucheary/.

obligations. Broad participation in the Singaporean market benefits the small firms that rely on a competitive choice of infrastructure.

Coordinate with Existing Frameworks and Internationally Recognised Standards

Regulatory approaches should prioritise coordination and clarity over new, centralised regimes. The Bill is intended to complement the Cybersecurity Act, which already provides for the designation and cybersecurity oversight of major foundational digital infrastructure service providers.[5] The two regimes should operate as a single coherent compliance architecture rather than as overlapping programmes.

Coordination should extend to the incident and disruption notification regime. Sections 15(c) and 16(1)(a)(iii) create duties to notify IMDA of cybersecurity incidents and service delivery disruptions. ACT welcomes section 16(2), which requires that codes of practice under the Bill not be inconsistent with codes or standards under the Cybersecurity Act. Building on that provision, IMDA should set clear thresholds and reasonable notification timelines, and should ensure that a single incident does not trigger duplicative or conflicting reports across the two regimes.

Allocate Obligations According to Operational Control and the Ability to Mitigate Risk

ACT urges MDDI and IMDA to align with the concept of shared responsibility across the digital infrastructure value chain. The ecosystem includes data centre operators, cloud infrastructure providers, application developers, customers, equipment owners, and end users. Not all actors have visibility into or control over how systems, equipment, and workloads are configured or used in practice. Assigning liability broadly without regard to control or context creates incentives to limit functionality and access rather than improve security or sustainability. Obligations should be allocated based on who can mitigate risk. Specifically, those in the value chain with the ability to minimise risks based on their knowledge and ability to mitigate should have appropriate incentives to do so.[6]

Information requests, audits, and emergency measures should be necessary, targeted, and proportionate to the regulated service and risk. In particular, coverage inquiries under section 14, compliance information requests under section 41, audits and directions under section 17, and emergency measures under section 18 should each be confined to what the regulated service and risk require. Such measures should protect customer data, source code, security architecture, vulnerability information, trade secrets, and legally privileged material. ACT notes that Section 18 is particularly broad, and appears to compel information about the design, configuration, and operation of systems, and override contractual and confidentiality obligations while preserving only legal privilege. Where these powers reach a regulated provider, they may sweep in the data, source

[5] Cybersecurity Act 2018, Part 3D (Singapore), https://sso.agc.gov.sg/Act/CA2018?ProvIds=pr3-&ValidDate=20251031.
[6] Association for Competitive Technology, AI Roles & Interdependencies Framework (May 2024), https://actonline.org/wp-content/uploads/ACT-AI-Roles-Interdependencies-Framework-final-text-May-2024-UK-English.pdf.

code, and trade secrets of that provider's downstream customers, many of which are small businesses. IMDA and the Minister should therefore exercise these powers only where necessary and proportionate, confine them to what a threat requires, and give affected parties notice and an opportunity to protect confidential material.

Assess Downstream Effects on Capacity, Affordability, and Competition

MDDI and IMDA should assess whether a proposed sustainability requirement could reduce cloud or colocation capacity, increase prices for smaller customers, limit specialised or high-performance workloads, restrict provider choice, or discourage investment in Singapore. The Part 4 licensing regime gives IMDA significant levers over both capacity and cost, including facility-level power usage effectiveness and water efficiency requirements, the allocation of limited data centre capacity through the competitive and non-competitive processes in section 22(4), and licence conditions under section 25(3) that can require low-carbon energy projects, carbon-credit offsets, electricity-import arrangements, and caps on specified energy sources. The costs associated with these measures will inevitably flow downstream to the smallest cloud and colocation customers, who are least able to absorb them and least able to negotiate custom arrangements. ACT believes that sustainability and continued infrastructure growth should be treated as complementary objectives, and that the framework should preserve distributed and cross-border architectures that reduce single points of failure and should not indirectly require data localisation or prevent businesses from selecting the most efficient regional infrastructure for their needs. Latency-sensitive products that ACT members build, including telehealth, real-time logistics, interactive media, connected devices, and cloud-delivered security services, depend on data centre capacity being reasonably close to their users, so capacity-allocation and sustainability measures that concentrate or constrain capacity can disadvantage the distributed, edge, and smaller workloads that small firms rely on. Where capacity is allocated by reference to economic or strategic importance to Singapore, IMDA should ensure that smaller and edge workloads are not crowded out by large anchor tenants.

MDDI and IMDA's stakeholder engagement should not be limited to the largest regulated providers and their direct competitors. It should include application developers, connected-device companies, cloud customers, data centre tenants, startups, and other businesses that may experience indirect costs or unintended consequences. Smaller firms may require targeted outreach, short-form contribution options, workshops, and sufficient time to prepare responses if their perspectives are to be meaningfully captured. ACT welcomes the procedural safeguards already in the Bill, including the appeal to the Minister and the Appeals Advisory Panel under Part 5, the 28-day representation windows on modifications to licence conditions, and the 21-day notice before a financial penalty. Consultation on codes of practice and implementing instruments, and the benefit of these representation rights, should reach the downstream application developers, connected-device companies, and small cloud customers that a measure may materially affect.

Conclusion

ACT appreciates the opportunity to provide comments on the draft Digital Infrastructure Bill. We support Singapore's objective of strengthening the security, resilience, and environmental sustainability of the digital infrastructure on which its economy and society depend. These goals are important for the small and medium-sized technology companies we represent.

ACT stands ready to engage further and to share additional insights from the small business technology ecosystem as MDDI and IMDA finalise the Bill and develop its implementing instruments.

ACT encloses as an annex its recently-issued paper, *Small Businesses and the Data Center Economy*, which develops these demand-side and supply-side points in greater depth.

Sincerely

Brian Scarpelli
Senior Global Policy Counsel
Association for Competitive Technology

Kedharnath (Kedhar) Sankararaman
Policy Counsel
Association for Competitive Technology

APPENDIX

ACT Association for Competitive Technology

Small Businesses and the Data Center Economy

I. Introduction

Public discussion of the data center economy tends to center on a small number of large entities: the hyperscale cloud providers, the utilities that power them, and the multibillion-dollar campuses they build. That framing obscures the impacts on the nation's small software and connected-device innovators, a constituency that is just as essential to the data center economy on *both* the supply side and the demand side. A resilient, secure, and domestically grounded data center supply chain has become a national economic and security imperative, and America's small and medium-sized technology firms are central to meeting the challenge, both as suppliers of the software and devices these facilities depend on and as the innovators who put the resulting capacity to work.

ACT represents the global startup and small technology business community that drives the modern digital economy and fuels American competitiveness, growth, and job creation. ACT members implement, monitor, secure, and run data centers with the software and devices they build. And even more small businesses depend on the compute, storage, connectivity, and cloud services those facilities make possible in order to enter new markets, reach customers, deploy AI-enabled tools, and grow.

To explore small technology businesses' relationship to America's data center economy and related policies, this paper looks first at the barriers that small businesses face. Then, it looks at how small software and connected-device firms participate in the data center supply chain as providers of the software, sensors, and digital services that help build out and run these facilities. Finally, it explains why data center capacity has to be geographically distributed, and how small firms *use and benefit from* the resulting infrastructure to power the new cloud and AI processing capacity they need to compete.

II. Barriers Small Businesses Face

For all their importance to the data center economy, startups and small technology businesses face real and growing barriers to taking full part in it. As users of data center capacity, the smallest firms are the most dependent on affordable and accessible cloud and AI services, yet they are the least able to absorb rising costs or to wait out the permitting and construction delays that hold back new capacity. A large enterprise may negotiate customized cloud contracts, reserve compute, or build private infrastructure. A small developer generally cannot. When capacity concentrates in a few large hubs, latency-sensitive tools or services are left far from the customers they serve, and policies that drive up the cost of compute, energy, or cloud services weigh most heavily on the smallest firms. Cloud and AI adoption still lags among these firms, even though they have the most to gain from it.

As suppliers, the small software, sensor, and connected-device companies that help build and run these facilities must compete for data center work against far larger incumbents, and they are often overlooked in the procurement processes, incentive programs, and economic data that shape data center policy. Federal efforts built around large construction and equipment firms can leave little room for this smaller digital-supplier tier, even as demand for the tools it provides grows. Lowering

these barriers, on both the demand and the supply sides, is the aim of the recommendations later in this paper.

III. Small Businesses as Participants in the Data Center Supply Chain

Building and running a modern data center draws on a deep and diverse vendor base, and a growing part of it is software and connected-device work that ACT members build. According to the U.S. Census Bureau, spending on data center construction reached approximately $41 billion in 2025, up about 32 percent from the prior year and more than 340 percent from 2020.[1] Federal Reserve researchers similarly estimate that nominal spending on data center structures rose from about $10 billion in 2021 to about $40 billion in the first half of 2025 alone.[2] Total investment is far larger still once the digital layer (servers, networking gear, and the software that runs them) where ACT's members take part is taken into account. As increased capacity becomes available, the firms that supply a data center's software and connected devices, its monitoring tools, control systems, sensors, and management platforms capture a meaningful and growing share of the activity. Because so much of this layer is built by American small and medium-sized firms, a healthy domestic base of these suppliers is itself part of a secure and resilient data center supply chain.

The data center economy that ACT's members build on is large and growing fast. A 2026 PwC analysis estimated that the U.S. data center industry supported roughly 5.5 million jobs and contributed about $927 billion to GDP in 2024 with each direct data center job supporting several more across the wider economy.[3]

Small businesses increasingly supply the digital layer a modern data center cannot run without. They build the infrastructure-management software that tracks power and cooling, the monitoring and observability tools that flag problems before they cause outages, the environmental sensors and controls that keep equipment within tolerance, the security software that protects the facility and its tenants, and the predictive-maintenance and energy-optimization tools that hold operating costs down. Many of these vendors are small firms. As facilities expand, the demand for the more automated and more energy-conscious software and connected devices startups and small technology companies make will grow alongside them.

Once a facility is operational, much of the recurring value to digital economy firms flows through software and cloud-delivered services. Operators rely on monitoring, analytics, security, and

---

[1] U.S. Census Bureau, Value of Construction Put in Place. Data center construction spending reached approximately $41 billion in 2025, up roughly 32% year-over-year and more than 340% from 2020. The Census series excludes the cost of servers and racks but includes built-in cooling and electrical equipment. Available at https://www.census.gov/construction/c30/c30index.html.

[2] Board of Governors of the Federal Reserve System, "Estimating Aggregate Data Center Investment with Project-Level Data," FEDS Working Paper No. 2025-109 (2025), noting nominal spending on data center structures rose from about $10 billion in 2021 to about $40 billion in the first half of 2025, and that total investment substantially exceeds the structures themselves once high-tech equipment is included. Available at https://www.frbsf.org/research-and-insights/publications/board-of-governors/2026/01/estimating-aggregate-data-center-investment-project-level-data/.

[3] PwC, "Economic Contributions of Data Centers in the United States, 2017–2023," commissioned by the Data Center Coalition (2025). PwC subsequently updated these figures in May 2026 ("Economic Contributions of Data Centers in the United States," 2024 data), reporting that the industry supported approximately 5.5 million U.S. jobs and contributed roughly $927 billion to GDP in 2024. Available at https://www.datacentercoalition.org/reports-and-publications.

management tools delivered as subscriptions, and on the small developers who build integrations, dashboards, and automation on top of cloud platforms.

IV. Small Businesses as Users and Beneficiaries of the Data Center Economy

The larger and more transformative story is on the demand side. The data center economy is the physical underpinning of the more than $700 billion cloud computing industry that lets a small business reach enterprise-grade technology at scale.[4]

It is important for capacity to be physically close to its users. Network latency, the delay between a request and its response, grows with the distance data must travel, so the industry places edge facilities near the users and devices they serve rather than concentrating everything in a few low-cost hubs.[5] Because latency-sensitive products such as telehealth, real-time logistics, interactive media, cybersecurity services, and connected devices must respond in close to real time, the small firms that build them depend on having data center capacity reasonably close to their own customers.[6]

A distinct and often-overlooked group of beneficiaries is the independent software developers and small connected-device companies that build, deploy, and distribute their products through digital platforms.[7] These firms write code in cloud environments, host and distribute applications from cloud infrastructure, and rely on cloud-delivered services to reach users worldwide. Many have only a handful of employees and depend directly on accessible, affordable, and reliable data center capacity located close enough to serve their users responsively.

Before cloud services, a firm that needed serious computing power had to purchase, house, and maintain its own servers, a capital expense that put advanced capability out of reach for most small businesses. Cloud infrastructure converts that fixed cost into a pay-as-you-go operating expense and removes the need for on-premises hardware and the staff to run it. A two-person startup can now provision the same class of compute and storage that once required a dedicated server room, and it can scale capacity up or down as demand changes. For ACT's members, this shift from owning infrastructure to renting it is the single most important benefit of the data center economy. The pay-as-you-go cloud model removes the infrastructure barrier to entry and lets a small team enter markets that used to be closed to anyone without a large capital budget.

---

[4] Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Total $723 Billion in 2025" (Nov. 2024), forecasting worldwide end-user spending on public cloud services of approximately $723.4 billion in 2025, up from $595.7 billion in 2024, an increase of roughly 21.5%. Available at https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025.

[5] US Signal, "Does Data Center Location Matter for Cloud Services?" (2026). Available at https://ussignal.com/blog/does-data-center-location-matter-for-cloud-services/.

[6] Equinix, "What Is an Edge Data Center?" (2024). Available at https://blog.equinix.com/blog/2024/09/12/what-is-an-edge-data-center/. Atlas, "Edge Data Center Location Planning" (2026). Available at https://atlas.co/blog/edge-data-center-location-planning/.

[7] U.S. Bureau of Labor Statistics, Occupational Outlook Handbook, "Software Developers, Quality Assurance Analysts, and Testers" (2025), reporting approximately 1.7 million software developers employed in the United States in 2024, with overall employment projected to grow 15% from 2024 to 2034, much faster than the average for all occupations. Available at https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm.

Generative-AI-specific cloud services, which grew on the order of 140 to 180 percent year-over-year in 2025,[8] reach small firms almost entirely through data-center-hosted services. A firm with a handful of employees can now use AI for customer service, marketing, document processing, pricing, and analytics on a subscription basis without the data centers, specialized chips, or data-science teams that training and serving such models require. The data center economy is, in practical terms, the delivery mechanism that puts advanced AI within reach of the smallest innovators, and it is the capacity that ACT's members need to build the next generation of AI-enabled products.

Approximately 18 percent of U.S. firms reported using AI in at least one business function, a share that rose to roughly 32 percent when weighted by employment and that businesses expected to climb further within six months.[9] Federal Reserve researchers tracking the same period reported a comparable adoption rate and noted that firm AI use had grown sharply over the prior year.[10] Adoption still runs lower among the smallest firms, which is exactly where affordable, cloud-delivered tools matter most, because they let a company pick up advanced capabilities without building its own infrastructure.

The AI assistant, the algorithmic real-time marketing analysis tool, the e-commerce storefront, the cloud-hosted CRM, and other tools that small firms now rely on all run on servers sitting in a data center somewhere. For ACT's members, data center infrastructure is the foundation the rest of their business now sits on.

V. Policy Recommendations

In concert with state policies, federal policy to support the continued expansion of the American data center economy is critical to startup and small tech growth and job creation and should be a national economic and security imperative. ACT recommends:

- **Shaping data center infrastructure policy to support American small business innovators.** Federal efforts and programs should recognize that small software and device firms are primary users of data center capacity and should be designed so that capacity remains accessible to them.
    - **Permitting and siting predictability.** Predictable, transparent permitting brings new capacity online faster, which directly benefits the small software and connected-device firms that need affordable cloud and AI capacity to compete.
    - **Support for distributed and edge capacity.** Because latency requires capacity near users, policies that enable responsible data center development across more

[8] Synergy Research Group, chief analyst John Dinsdale, Q2 2025 commentary. Available at https://www.srgresearch.com/articles/q2-cloud-market-nears-100-billion-milestone-and-its-still-growing-by-25-year-over-year.

[9] U.S. Census Bureau, Business Trends and Outlook Survey, artificial intelligence supplement (data collected Nov. 2025 through Feb. 2026), reporting that approximately 18% of firms used AI in at least one business function, rising to about 32% on an employment-weighted basis, with adoption projected to reach 22% within six months. Available at https://www.census.gov/library/working-papers/2026/adrm/CES-WP-26-25.html.

[10] Board of Governors of the Federal Reserve System, Jeffrey S. Allen, "Monitoring AI Adoption in the U.S. Economy," FEDS Notes (Apr. 3, 2026), reporting that about 18% of firms had adopted AI as of year-end 2025 and that adoption grew sharply over the prior year. Available at https://www.federalreserve.gov/econres/notes/feds-notes/monitoring-ai-adoption-in-the-u-s-economy-20260403.html.

regions serve the latency-sensitive software and connected-device firms ACT represents, whose products must respond in real time, and they spread supplier opportunities to more communities at the same time.
    - **Affordable, reliable power and connectivity.** Because ACT's small business members are among the largest classes of data center users, policies that keep compute and energy costs reasonable directly protect their access. Regulatory approaches that raise the cost of cloud services fall hardest on the smallest users.
- **Small-business incentives.** Federal incentives, grants, or siting agreements supporting data center development should enable small software and connected-device suppliers to compete to provide the monitoring, security, and management technology these facilities depend on.
    - **Set-asides in existing programs.** Programs such as CHIPS Act extensions, Small Business Administration (SBA) loans, and U.S, Department of Agriculture (USDA) guaranteed loans should reserve a share for small software, sensor, and connected-device companies that supply data center monitoring, security, observability, and energy-management tools.
    - **Targeted tax credits and grants.** Tax credits, vouchers, or matching grants should support startups and small technology companies that are (1) developing and deploying edge computing solutions to support distributed capacity and help smaller firms compete, or (2) adopting cloud and AI services. These measures would lower barriers, especially for the smallest firms, where adoption currently lags.
- **Supporting a secure data center supply chain.** Federal data center policy should account for the American software developers and connected-device makers who supply the monitoring, control, security, and management layer that keeps these facilities running. Programs and data collection that track who benefits from data center investment should make this digital supplier tier visible. Efforts to expand domestic production of the sensors, devices, and components that data centers and connected products rely on create opportunities for small connected-device makers and strengthen the supply-chain resilience the broader app economy depends on.
- **Fact-based public engagement.** Federal leadership in surfacing rigorous economic data on data centers, including the role of small software and connected-device firms as both suppliers and users, supports informed local decision-making and a fuller public understanding of who the data center economy serves. More work is needed to quantify startup and small technology businesses contributions (both supply and demand) and cost impacts to inform better policymaking.

VI. Conclusion

Countless small software and connected-device firms help instrument and run these facilities and depend on the cloud and AI capacity those facilities provide to start up, operate, reach customers, and now to build AI-enabled products at scale. A strong, secure, and domestically grounded data center supply chain is a national economic and security imperative, and these small firms are central to meeting it. Federal policy that recognizes both roles will produce an American data center economy that supports the next wave of American innovation.