Billing Code 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 240823-0225]

RIN 0660-XC062

Request For Comments on Bolstering Data Center Growth, Resilience, and Security

AGENCY: National Telecommunications and Information Administration, Department of Commerce.

ACTION: Notice, Request for Comment.

SUMMARY: The National Telecommunications and Information Administration (NTIA) hereby requests comments on the challenges surrounding data center growth, resilience and security in the United States amidst a surge of computing power demand due to the development of critical and emerging technologies. This request focuses on identifying opportunities for the U.S. government to improve data centers' market development, supply chain resilience, and data security. NTIA will rely on these comments, along with other public engagements on this topic, to draft and issue a public report capturing economic and security policy considerations and policy recommendations for fostering safe, secure, and sustainable data center growth.

DATES: Written comments must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: All electronic public comments on this action, identified by Regulations.gov docket number NTIA–2024–0002, may be submitted through the Federal e-Rulemaking Portal at www.regulations.gov. The docket established for this request for comment can be found at www.regulations.gov, NTIA–2024–0002. Click the ‘‘Comment Now!’’ icon, complete the required fields, and enter or attach your comments. Additional instructions can be found in the ‘‘Instructions’’ section below after ‘‘Supplementary Information.’’

All comments received are a part of the public record and will generally be posted to Regulations.gov without change. All personal identifying information (e.g., name, address) voluntarily submitted by the commenter may be publicly accessible.

If you would like to submit business confidential information, please clearly identify any business confidential portion of a comment at the time of submission, file a statement justifying nondisclosure and referring to the specific legal authority claimed, and provide a non-confidential version of the submission.

For comments submitted electronically containing business confidential information, the file name of the business confidential version should begin with the characters “BC.” Any page containing business confidential information must be clearly marked “BUSINESS CONFIDENTIAL” on the top of that page. The corresponding non-confidential version of those comments must be clearly marked “PUBLIC.” The file name of the non-confidential version should begin with the character “P.” Any submissions with file names that do not begin with either a “BC” or a “P” will be assumed to be public and will be made publicly available through https://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Please direct questions regarding this Request for Comment to Travis Hall at thall@ntia.gov with ‘‘Bolstering Data Center Resilience and Security Request for Comment’’ in the subject line, or if by mail, addressed to Travis Hall, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Room 4725, Washington, DC 20230; telephone: (202) 482–

3522. Please direct media inquiries to NTIA's Office of Public Affairs, telephone: (202) 482–7002; email: press@ntia.gov.

SUPPLEMENTARY INFORMATION

Background and Authority

Critical and emerging technologies like artificial intelligence (AI) have accelerated demands for more computing infrastructure. Powering these transformative technologies are data centers - facilities that house computing machines and related hardware components that process, store, and transmit large amounts of data - and the telecommunication infrastructure enabling information processing.[1]

Data centers are important enablers for economic growth and technological development. Their capabilities for data processing, ubiquitous connectivity, secure storage, cost-efficiency, and economy-wide job creation, among others, yield substantial benefits.

There are approximately 5,000 data centers in the United States, and data center demand is projected to grow domestically by roughly nine percent year over year through 2030.[2,3] Driven primarily by hyperscalers,[4] the total capacity of all data centers, including on-premise and colocation, is expected to rise steadily.[5] The expected growth in computing demand, and

[1] 42 U.S.C. § 17112(b)

[2] Cloudscene, "Data Centers in the United States" (March 2024) https://cloudscene.com/market/data-centers-in-united-states/all?trk=public_post_comment-text

[3] McKinsey, "Investing in the rising data center economy" (January 2023). Demand is measured by power consumption to reflect the number of servers a data center can house. Demand includes megawatts for storage, servers, and networks. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/investing-in-the-rising-data-center-economy.

[4] The term "hyperscale" data centers refer to data centers facilities comprising of 10,000 square foot/5,000-server facilities to colossal campuses with individual buildings over one million square feet, each containing hundreds of thousands of servers. *See* In-Q-Tel, "Workshop on Cloud, Data Centers, and Great Power Competition," (November 2023). https://assets.iqt.org/pdfs/Workshop-Report_Data-Centers_Nov-2023.pdf/web/viewer.html

[5] Synergy Research Group, "On Premise Data Center Capacity Being Increasingly Dwarfed by Hyperscalers and Colocation Companies," (July 2023). https://www.srgresearch.com/articles/on-premise-data-center-capacity-being-increasingly-dwarfed-by-hyperscalers-and-colocation-companies

resulting demand for data centers, present challenges and opportunities for data center operators in balancing market growth, supply chain resilience, and data security. For example, energy supply, restrictive permitting, skilled workforce shortages, and land unavailability may present localized growth challenges in certain domestic markets.[6] However, the increase in compute demand may also present opportunities to collaborate on public and private sector measures (e.g., infrastructure investments, workforce development programs) to catalyze data center growth, enable innovation, and foster economic development and global market leadership.

The continued growth of the U.S. data center industry hinges on resilient supply chains, access to power, trusted Information and Communications Technology and Services (ICTS) equipment, and a skilled workforce, among other factors. Powering and cooling data centers is energy-intensive: data centers physically located in the United States consumed more than four percent of the country's total electricity in 2022, with projections suggesting the share may increase up to nine[7] percent by 2030[8]. The increase in demand is incentivizing data center developers and utilities to maximize utilization of existing power grid infrastructure and water usage, with some data center operators pursuing alternatives to the grid, such as on-site energy generation and power grid infrastructure.[9] Outfitting new and existing data centers also requires a range of critical information technology (IT) and operational technology (OT) components -

[6] Global Data Center Trends 2023. (2023, July 14). https://www.cbre.com/insights/reports/global-data-center-trends-2023; CBRE. https://www.cbre.com/insights/reports/global-data-center-trends-2023

[7] SemiAnalysis, "AI Datacenter Energy Dilemma - Race for AI Datacenter Space," (March 2024). https://www.semianalysis.com/p/ai-datacenter-energy-dilemma-race

[8] Aljbour, Jordan, Tom Wilson, and Poorvi Patel. "Powering Intelligence: Analyzing Artificial Intelligence and Data Center Energy Consumption." White Paper. EPRI, May 2024. https://restservice.epri.com/publicdownload/000000003002028905/0/Product.

[9] Mondal, S., Fashat, B. F., Rajbongshi, D., Mohammad Masum, K. E., & Islam, M. M. (2023). GEECO: Green data centers for energy optimization and carbon footprint reduction. Sustainability, 15(21), 15249. doi: https://doi.org/10.3390/su152115249

semiconductors, chips, fiber optic cables, networking equipment, and more.[10] Lack of access to trusted equipment and skilled workforce shortages could limit both cyber and physical security functions necessary to protecting critical infrastructure operations.[11]

As the adoption of critical and emerging technologies like AI grows, with data centers playing a pivotal role in training and deploying AI models, there may be an amplified need to fortify security measures within these facilities. Heightened safeguards and robust security protocols may be necessary to protect the large volumes of data being processed and analyzed in support of cutting-edge applications.[12] Understanding current data security practices and gaps will be necessary in continuing to promote and maintain an open, inclusive, secure, and resilient digital ecosystem.

As part of the Department of Commerce's mission to create the conditions for economic growth and opportunity, and in line with its statutory role as the President's principal advisor on telecommunication and information policy, the National Telecommunications and Information Administration (NTIA) seeks input on the potential risks, benefits, and implications of the anticipated growth in the data center sector, and the appropriate policy and regulatory approaches to foster sustainable, resilient and secure data center growth. The responses to this request will help inform a report that will address the hurdles and opportunities for this vital industry sector and will provide policy recommendations for actions the federal government can take to help

[10] U.S. Department of Commerce and Department of Homeland Security, "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry," (February 2022). https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_0.pdf

[11] U.S. Department of Homeland Security, "Advisory Memorandum on Ensuring Essential Critical Infrastructure Workers' Ability to Work During the Covid-19 Response," (August 2021). https://www.cisa.gov/sites/default/files/publications/essential_critical_infrastructure_workforce-guidance_v4.1_508.pdf

[12] *See* Tim Fist, Michael Depp, and Caleb Withers "Response to OSTP "National Priorities for Artificial Intelligence Request for Information." *Center for New American Security* (July 20, 2023). https://www.cnas.org/publications/commentary/ostp-national-priorities-for-artificial-intelligence

foster the sector’s growth in a manner that is safe, sustainable, secure, and in service of the American people.

NTIA is issuing the Request for Comment in coordination with the Department of Energy (DOE), given DOE’s mission to ensure American’s security and prosperity through addressing energy challenges with science and technology solutions. Given the significant energy needs of data centers, DOE has a strong interest in understanding and supporting growth in the data center sector (See https://www.energy.gov/policy/articles/clean-energy-resources-meet-data-center-electricity-demand). DOE may use the responses from the request to inform the development of strategies, programs, and other actions to support deployment of technologies and solutions to address data center energy needs.

Instructions for Commenters

Through this Request for Comment, we hope to gather information on the following questions. These are not exhaustive, and commenters are invited to provide input on relevant questions not asked below. Commenters are not required to respond to all questions. When responding to one or more of the questions below, please note in the text of your response the number of the question to which you are responding. Commenters should include a page number on each page of their submissions. Commenters are welcome to provide specific actionable proposals, rationales, and relevant facts.

Questions

1. What current and future challenges and opportunities do commercially owned or operated data centers in the United States face in supplying computing power required by critical and emerging technologies, such as AI?

2. What are critical market considerations for the data center industry seeking to modernize or expand their footprint?

    a. Please describe key considerations such as: access to key markets, customer demand, access to renewable energy, data residency requirements, available high-speed broadband telecommunications infrastructure, access to workforce, government incentives, land or water availability, power grid connectivity, low power costs, or any other key considerations.

    b. What role does competition between hyperscalers play in the modernization or expansion of the data center industry? Are there barriers for new hyperscalers entering the marketplace? Can those barriers be reduced to promote competition? What are the barriers for customers to switching data centers service providers?

    c. What key regulatory barriers exist at the federal, state, local, tribal, and territorial level?

    d. What existing private or public programs, initiatives, or incentives effectively drive data center modernization or investment within the United States?

    e. What role or actions, if any, should be taken by the private sector, civil society or the U.S. government to mitigate potential barriers to, or foster opportunities for, data center market entry, growth and modernization?

    f. What are the causes of foreign, exogenous forces, if any, pulling data center market opportunity away from the United States?

    g. How might data centers' modernization or investment affect other markets and industries?

h. What role or actions, if any, should be taken by the private sector, civil society or the U.S. government to address any inefficiencies due to market externalities or market failures?

3. As demand for computing power and data processing increases, what are the potential societal impacts (e.g., communities, environment, customers) — both positive and negative — of data center modernization or investment?

   a. How might rising demand for data centers affect operational costs (i.e., through increases in land, energy, water, and equipment costs)? Is an imbalance between demand and supply expected? How might changes to operational costs disproportionately affect small and medium-sized businesses compared to larger enterprises?

   b. How might growth in the U.S. data center industry result in increases in energy demand? How might it impact the environment? How can data center-related greenhouse gas emissions be managed to address concerns related to climate change?

   c. How might data centers' modernization or investment affect disadvantaged communities or groups, including rural communities, in their sites of operation?

   d. What role or actions, if any, should be taken by the private sector, civil society or the U.S. government to address any outcomes stemming from data center modernization or investment in disadvantaged communities or small and medium-sized businesses?

4. What are the supply chain risks, vulnerabilities, and threats to data center modernization, investment, growth or continuity?

a. What supply chain interdependencies are critical to ensuring availability of the critical IT/OT components within data centers? What IT/OT equipment supply chain shortages, if any, might hinder the development of data centers in the United States?

b. Are data centers experiencing shortages of fiber optic cable, chips, or any other equipment that may hinder data center development in the United States?

c. How are data centers approaching and planning for the transition to modern data center models and architectures (e.g., edge computing, AI-enabled, software-defined infrastructure, or digital coherent optics)?

d. How prevalent is the use of open-source software in critical IT/OT systems in data centers in the United States? What steps or processes are undertaken by data center operators to ensure the quality and security of the open-source software?

e. Who are the major suppliers (both foreign and domestic) of data center hardware, software, and services? What can the U.S. government do to bolster smaller suppliers?

f. Do any suppliers based outside of the United States or with relevant manufacturing operations occurring outside of the United States play systemic roles in providing components utilized in U.S. data centers?

5. What requirements, standards, and supply chain risk management best practices do data centers operators or customers have in place?

   a. How do data centers operators or customers ensure that untrusted or counterfeit IT/OT components do not make their way into U.S. data center facilities?

   b. What auditing processes for IT/OT equipment are used by data center operators or customers (i.e., software bill of materials)? Are there barriers to performing IT/OT equipment audits?

   c. How do data center operators or customers vet IT/OT equipment suppliers, providers or vendors?

   d. What controls do data centers operators or customers have in place to monitor vulnerabilities in legacy equipment?

   e. How do data centers perform contingency planning to ensure supply chain resiliency in the face of disruption? How do data center operators select diverse geographical areas of operation to ensure business continuity? How do data centers integrate alternative power sources in case of disruption, including backup generators that can power the data center up to 30 days?

6. Are there workforce challenges inhibiting growth in the data center industry? Is the data center industry experiencing a shortage of network engineers, cybersecurity professionals, construction workers, or any other types of professionals?

   a. What opportunities exist for partnering or collaborating with the U.S. government, including federally funded research and development centers (FFRDC) and University Affiliated Research Centers (UARCs), to help address data center challenges to accessing skilled workforce?

7. What challenges do data centers face in accessing power for their facilities? What novel solutions are data center operators exploring or implementing to ensure access to power?

   a. Can data centers get sufficiently reliable power from utilities? How do data centers decide whether to install backup power, and how do they design and size backup power sources?

b. What initiatives are data centers exploring as alternatives to grid connected power and traditional cooling solutions in their facilities? Are data centers facing obstacles in these efforts?

c. What initiatives are data centers exploring (e.g., net zero efforts) to mitigate greenhouse gas emissions from energy use? Are data centers facing obstacles in these efforts?

d. What are the most effective innovations in data center cooling / reduction in power usage effectiveness (e.g., networking innovations, silicon photonics)?

e. Can data center backup power generation be used to participate in utility demand response programs?

f. Are there opportunities for new tariff structures to help connect large loads to the grid while mitigating the risk of cost shifts to other electricity customers?

8. What voluntary guidelines, domestic regulations, or frameworks are currently in place or should be implemented to help manage data security risks in data centers while also maximizing the benefits of secure data processing and storage?

    a. What security controls do data center operators have in place to protect customer data? What governance mechanisms do data centers use to oversee compliance? How could data center operators or customers improve security controls?

    b. What are the key obstacles for data center operators to improve security? Are factors like competitive pressure, lack of demand, lack of cybersecurity professionals, or lack of security frameworks or regulations obstacles to improving security?

    c. Data center operators and cloud service providers often rely on a shared responsibility model to outline security responsibilities between the customer and the data center or cloud service provider.[13] How could data center operators, cloud service providers or customers improve the shared responsibility model?

d. How do data center operators address cyber incidents and breaches? Are there any cybersecurity incident reporting measures that would help increase data center security? What governmental support would help operators and developers achieve greater security?

e. What tools are data center operators using or experimenting with to ensure next generation data security practices are scalable?

f. What kind of entities should take a leadership role in sharing information about data security risks to data centers and solutions to addressing them? Should the type of entity vary by sector, and, if so, how?

9. What are the security considerations for data centers running or training frontier AI models[14] or integrating AI capabilities within existing infrastructure?

   a. Have data centers implemented any novel physical or cybersecurity measures in data centers' running or training frontier AI models that they have not implemented for other data center applications?

   b. What cybersecurity requirements, technical controls, or risk assessments should be implemented to ensure adequate data security practices in data centers that run and train frontier AI models? Should these requirements scale for less powerful versus more powerful AI models, and if so, how?

[13] *See* NIST Special Publication 500-292 "NIST Cloud Computing Reference Architecture," (2011) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

[14] The term "frontier AI models" refers to models that are overall more powerful than any currently released models (e.g., GPT-4, Claude 2, PaLM 2, Titan and, in the case of image generation, DALL-E 2). *See* White House, "Ensuring Safe Secure and Trustworthy AI," (July 2023). https://www.whitehouse.gov/wp-content/uploads/2023/07/Ensuring-Safe-Secure-and-Trustworthy-AI.pdf

c. How economically feasible is it for data center operators to maintain physical separation between infrastructure used for frontier AI training or for inference and other applications? What effects, if any, would this achieve beyond logical separation?

d. Are there any economic or technical reasons not to keep highly sensitive data, or frontier AI model weights, encrypted at rest, in use and in transit? Are there economical or technological barriers that would hinder the deployment of other data security measures that would protect highly sensitive data, such as frontier AI model weights?

e. What data security measures are data centers implementing as they integrate AI applications and capabilities within their existing infrastructure (e.g., power management, energy efficiency)?

10. What training tools and exercises do data centers use to train personnel and validate the efficacy of their data security posture?

a. What forms of on-the-job data security training do data centers provide to their staff?

b. How do data centers evaluate their employees' data security competencies? Describe any industry certifications that data center operators prioritize to indicate competence in data security.

c. Describe how data centers work with third parties in red-teaming efforts to simulate outside attacks. How often do data centers provide third parties' access? What level of access do data centers provide to third parties?

11. What role or actions, if any, should be taken by the Department of Commerce and, more generally, the federal government, to address the challenges to and opportunities for fostering the development of data centers?

Dated: September XX, 2024

Stephanie Weiner,

Chief Counsel, National Telecommunications and Information Administration.