National Electrical Manufacturers Association

November 4, 2024

Via Federal eRulemaking Portal https://www.regulations.gov
Docket Number NTIA-2024-0002

Ms. Stephanie Weiner
Chief Counsel, National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave.; Room 4725
Washington, DC 20230

Re: Request for Comments on Bolstering Data Center Growth, Resilience, and Security

Dear Ms. Weiner:

The National Electrical Manufacturers Association (NEMA) is the leading trade group representing America's electroindustry. Our more than 300 members manufacture safe, reliable, efficient and secure products that serve key markets, including building infrastructure, building systems, and utility products and systems. Electromanufacturers serve as the industrial backbone to the nation's electric grid, providing the components that are essential and critical for electrification, power resilience, and economic advancement.

NEMA welcomes this joint Request for Information (RFI) by the National Telecommunications and Information Administration (NTIA) and the Department of Energy (DOE) into the economic and security policy considerations and future development of appropriate policies needed to foster safe, secure, and sustainable data center growth. Data centers, from smaller "edge" facilities to the "hyperscale" installations supporting cloud and big data storage, play a positive and integral role in the U.S. economy by enabling machine learning technologies and systems to comprehend the vast amount of information stored within them.

Current-state artificial intelligence (AI) models, and the near-promise of even more advanced large-language models and quantum computing power, are essential to sustaining a free and open society where information is available to all. Given the data

center industry's rapid growth and imminent impact on various critical infrastructure sectors, including energy, critical manufacturing, and communications, it is both appropriate and necessary to assess the proper role of federal government involvement in this space. An appropriate and clearly defined balance of engagement, leadership, and partnership between the public sector, the data center industry itself, supply chain vendors, power utilities, and other key stakeholders will help ensure effective and sustainable development of these economic assets as well as predict and meet future needs and challenges.

Electromanufacturers produce electric grid technologies and critical components that electric utilities need to reliably generate, transmit, and distribute energy to customers in their service area. Traditional customers have generally included residential, commercial, and industrial/manufacturing entities, each of which have varying energy load demands. However, the rapidly growing data center industry is creating load stipulations that are exponentially greater than these traditional end-users, creating both opportunities and challenges for policymakers, utilities, and supply chain vendors.

To satisfy their energy needs, data centers have begun to build and incorporate localized energy generation and distribution solutions. As such, owners and operators of these facilities are now direct consumers of grid technologies and critical components. These new entities create the potential to yield creative and innovative solutions to energy efficiency and power management, as well as accelerate the research and development of grid technologies, including battery storage, microgrids, and smart-grid applications. NEMA and the electroindustry will continue to engage with all partners to determine how manufacturers can contribute to advancing the goals of the national energy transition while enabling this rapidly developing industry.

Furthermore, as this industry grows and becomes even more integrated with the energy sector, standardization of components and technologies will be necessary to ensure supply chain safety, security, and reliability. Based on nearly a century of experience developing standards across the electroindustry as an ANSI-accredited Standards Development Organization, NEMA is advancing standards, codes, and other technical guidance to better enable high-performance data centers to consume less energy, generate local or on-site energy, and store electricity.

Many of NEMA's policy priorities for the successful energy transition are also relevant to the federal government's goals for assuring safe, secure, and sustainable data center growth. **These priorities include strengthening the future workforce, supply chain strength and integrity, multi-sector collaboration, and grid technology innovation**.

Strengthening the Future Workforce

Like many other U.S. economic sectors, the electroindustry is focused on attracting, developing, and strengthening the necessary skilled and technical workforce needed to produce components and technologies that enable the grid. Regarding the development, construction,

and powering of data centers, federal partners can help address current gaps by fostering meaningful, inclusive discussions among supply chain electromanufacturers, data center owners and operators, electric utilities, and relevant educational and training institutions, among others, which produce and incentivize actionable implementation plans that will increase and diversify the talent pipeline. These plans should prepare future workers to serve in multiple industries where data analytics, technology expertise, and critical thinking skills are valued.

Supply Chain Strength and Integrity

Just as for any critical sector, sustainable growth for data centers relies on reliable and abundant supply chains. Given current labor and material shortages, which are leading to extensive lead times for critical grid components, including large-power and distribution transformers, the federal government and its partners should continue to focus on implementing constructive policies and removing barriers, which will increase the volume and successful outputs of domestic manufacturing.

In September 2024, the National Infrastructure Advisory Council (NIAC) published *Addressing the Critical Shortage of Power Transformers to Ensure Reliability of the U.S. Grid,* *which* included a series of recommendations to address transformer supply chain constraints. NEMA, alongside utilities and DOE, contributed to the development of these recommendations, which included bolstering workforce capabilities (as noted above), long-term contracting, product standardization, sufficient and purposeful tax incentives, and the creation of a "virtual reserve" where the federal government is a buyer of last resort to create long-term production certainty. NEMA encourages NTIA to engage with

DOE and the other participating entities to determine the best methods of implementing the report's recommendations.

In response to specific RFI questions concerning supply chain risks management and best practices, NEMA offers the following:

- **What supply chain interdependencies are critical to ensuring availability of the critical IT/OT components within data centers?**

  There are multiple interdependencies, including materials sourcing, logistics, transportation, manufacturing capabilities, vendor relationships, regulatory compliance, technology integration, and access to skilled workers.

- **What IT/OT equipment supply chain shortages, if any, might hinder the development of data centers in the United States?**

  NEMA members monitor potential shortages of semi-conductor components, servers, cooling systems, network equipment, backup systems, shortage devices, microchips, and trusted platform modules.

- **How prevalent is the use of open-source software in critical IT/OT systems in data centers in the United States?**

  Open-source software is very prevalent and critical to the development of interoperable IT/OT systems. It is cost-effective due to collaboration and community support; continued and expanded use of open-source software is necessary to ensure added interoperability. Data centers, manufacturers, utilities, and government should
  continue to work together on quality and security assurance in this space. This includes ensuring only vetted individuals can submit specific open-source software to development and hosting communities. Further, there is value in continuing work on software and hardware bills of materials (SBOM and HBOM).

- **What steps or processes are undertaken by data center operators to ensure the quality and security of the open-source software?**

  NEMA members have experienced data centers undertaking several processes to ensure open-source software quality and security, including security assessments, testing, validation, configuration management, monitoring, logging, patch management, training, access controls, increased governance, and staff/vendor training.

- **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?**

  Robust audit processes for suppliers, enforcing "root of trust" and code signing requirements for products, and continued evolution of SBOM and HBOM processes can help prevent untrusted and/or counterfeit products from being placed in or interacting with domestic data center facilities. It is also important to request background checks that include screens for financial stability. AI-enabled software can already aid continuous supplier assessments and audits. Baseline tactics that should be broadly encouraged and adopted include product evaluation and testing, paired with risk management practices and contingency plans.

- **What auditing processes for IT/OT equipment are used by data center operators or customers (i.e., software bill of materials)?**

  Auditing processes include but are not limited to:

  - SBOMs
  - Hardware Inventory audits
  - Secure baseline config audits
  - Vulnerability assessment and management
  - Compliance audits against standards, regulations, and frameworks
  - Incident Response Review

- **Are there barriers to performing IT/OT equipment audits?**

  Intellectual Property disagreements and geopolitical conflict can hinder effective IT/OT equipment audits. Other challenges include diverse and extraordinarily complex operating environments, resource and training limitations, confidentiality and data privacy concerns.

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

  Vetting methods include but are not limited to:

  - Background Checks including financial stability
  - Continuous Supplier Assessments
  - Continuous Supplier Audits
  - Review of quality and compliance
  - Product evaluation and testing
  - Risk Management practices and contingency plans

Multi-Sector Collaboration

Data centers can be viewed as critical infrastructure components which enable the functions of more traditionally recognized critical infrastructure sectors, including communications, defense, and energy. The federal government should leverage the appropriate Sector Risk Management Agencies (SRMA) and their federally chartered Sector Coordinating Councils (SCCs) to foster high-level and constructive information exchanges with data center owners and operators. These exchanges should identify current and near-term holistic challenges that data center growth and evolution will present to those critical infrastructure sectors and develop practical and actionable plans to address those challenges. These plans should also identify where Congressional authorization is needed to properly address challenges.

At a minimum, DOE, the SRMA for the energy sector, should partner with the Department of Homeland Security (DHS), the SRMA for the Critical Manufacturing, Information Technology, and Communications sectors. This partnership should ensure that the SCCs can foster greater cooperation and information sharing regarding data centers, including areas of concern related to supply chain, growth, sustainability, reliability, cybersecurity and physical security.

Grid Technology Innovation

According to the Electric Power Research Institute, energy consumption from data centers alone is projected to consume at least 9% of all domestic power by 2030.[1] In addition to significantly and quickly increasing the amount of generation and transmission to meet this demand, adopting innovative technologies along the grid will be critical to ensure maximum energy efficiency and reduce load loss. Government-led discussions, partnerships, and policies should seek to further both transmission and distribution grid innovation and the deployment of products, technologies, and systems that enhance the reliability and deliverability of electric power to end uses.

Most data center energy demand stems from server consumption and cooling. Data centers have significant opportunities to deploy demand-based grid flexibility and energy efficient solutions, such as broadening operating temperature limits, scheduling AI model training for off-peak hours, and using power-cycler software to power-down idle servers, when possible. Time of use rates enhance the opportunities to deploy these types of tactics and technologies.

Government and private sector partnerships should highlight successes to better enable the next generation of data centers to plan for more efficient operations, whether in the components and software they choose or in the rate structures they negotiate with incumbent utilities. The federal government should continue to prioritize research and development dollars and activities aimed at solving data center power needs and approaches that maximize the efficient use of power at these facilities.

As data centers are seeking their own generative sources of energy apart from established electric grids, microgrids, distributed energy resources (DER), and smart-grid technologies can help increase electric efficiencies and reliability. Further, the encouragement of grid enhancing technologies (GETs) and enhanced wiring techniques can help magnify the efficiency of electric transmission networks to supply load from generation sources located at a distance from data centers.

Thank you for the opportunity to share NEMA's member perspectives. NEMA and its members look forward to engaging in continued discussions about strategies and policies that will ensure data centers, the energy sector, and the electroindustry can successfully navigate the energy transition and continue to support a strong national economy and a resilient energy grid. Please direct follow up questions about NEMA's response to this RFI to Laura Schepis, Executive Director, Grid Policy at laura.schepis@nema.org.

Sincerely,

Laura M. Schepis
Executive Director, Regulatory and Industry Affairs, The Grid
National Electrical Manufacturers Association
Laura.schepis@nema.org

---

[1] https://www.epri.com/research/products/000000003002028905