Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Request for Comments on Bolstering Data Center Growth Resilience and Security	)	Docket No. 240823-0225
	)	
	)	
	)	

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA") appreciates the opportunity to provide input to NTIA pursuant to the Request for Comments on Bolstering Data Center Growth Resilience and Security ("RFC"). TIA is a U.S.-based trade association and Standards Developing Organization ("SDO") that represents more than 400 trusted, global manufacturers of telecommunications equipment and services. TIA members design, produce, market, and manage the information communications technology ("ICT") equipment and services that connect Americans to high-speed broadband networks.

SDOs like TIA have a significant role to play in bolstering data center growth, resilience, and security by providing voluntary guidelines, best practices, and frameworks used for conformity assessment and certification. TIA recommends that the Department of Commerce, and more generally the federal government, act to address the challenges and opportunities for

fostering the development of data centers by promoting and encouraging efforts by SDOs that foster sustainable, resilient, and secure data center growth.[1] Specifically, TIA recommends that:

1) U.S. government ("USG") data center customers should require the use of certain voluntary consensus standards ("VCS") along with certifications related to those VCS;
2) USG should establish clear, transparent expectations regarding potential supply chain threats;
3) USG should consider how TIA industry programs might support workforce development, quality improvement, and supply chain security;
4) USG agencies and programs provide financial support to individuals and organizations that operate and contribute to data center standardization efforts; and
5) The Office of the United States Trade Representative should support policies that facilitate cross border data flows.

Standards support data center growth, resilience, and security

NTIA's RFC asks multiple questions about existing requirements, standards, best practices, voluntary guidelines, and frameworks that are used by data center operators and their customers.[2] This focus on standards is positive and can accelerate data center growth and performance establishing common benchmarks and vocabulary for performance across various metrics. To the extent that this RFC leads to specific government action, we believe that it would be appropriate for NTIA to use or otherwise reference VCS in line with existing federal

[1] NTIA RFC Question 11: "What role or action, if any, should be taken by the Department of Commerce and, more generally, the federal government, to address the challenges and opportunities for fostering the development of data centers?"
[2] NTIA RFC Questions 5 and 8.

guidance. Specifically, OMB Circular A-119 states that "federal agencies must use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities." Leveraging VCS standards developed by the private sector lowers costs incurred by the federal government, and it allows agencies to leverage and compare against benchmarks widely used across the private sector. Using VCS standards developed on a consensus basis by SDOs – as opposed to standards developed by consortia that may not include procedures relating to openness, balance, due process, appeals, and consensus – also ensures that the outcome reflects a broad range of stakeholder input.

TIA is an ANSI-accredited SDO that develops VCS that are widely used as voluntary guidelines, best practices, and frameworks by technology companies including data center operators and their customers. One specific VCS is directly relevant to NTIA's inquiry – **ANSI/TIA-942: Telecommunications Infrastructure Standard for Data Centers.**[3] Developed by TIA's TR-42 Committee,[4] ANSI/TIA 942 provides a comprehensive framework for the design and installation of data center infrastructure including cabling, cooling, power, architecture, physical security, fire protection, safety, and monitoring ensuring consistency across data centers. It offers a scalable design that ensures data centers can adapt to growth and technological advancements. The standard defines four rating categories for redundancy and fault tolerance that allows organizations to audit and certify their data centers to meet their operational requirements while promoting resiliency.

Additionally, TIA oversees an ANSI/TIA-942 certification program that, since 2021, has licensed qualified auditors to certify data centers to the standard. Certification bodies audit data

[3] ANSI/TIA-942 Standard, Telecommunications Industry Association, https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/

[4] In addition to ANSI/TIA-942, TR-42 develops other VCS for ICT infrastructure such as cabling, bonding, grounding, labeling, pathways, etc. also widely used in data centers and other ICT spaces.

center designs and implementations to ensure they meet one of four ANSI/TIA-942 ratings. Data centers need to be recertified in subsequent years to confirm they are still compliant, and there are currently eight ANSI/TIA-9423 certification bodies. There have been over five hundred data centers certified in over fifty countries, and fourteen data centers in the U.S. alone. The speed of certifications is also increasing, and there have been over two hundred certifications so far in 2024.

Assessments and certifications are important tools to ensure data centers meet rigorous industry standards. They provide multiple benefits including quality assurance, security, compliance, operational efficiency, resilience, and customer trust. The U.S. government can support American leadership in this industry by requiring that data centers they build or utilize are certified to industry standards like ANSI/TIA-942. Such a step would be in line with global practice, as many governments around the world have required that certain data center infrastructure is certified to ANSI/TIA-942.[5]

USG should establish clear, transparent expectations regarding potential supply chain threats

With regards to ensuring resilient supply chains for equipment that goes into data centers, our members are keenly aware of the due diligence the ICT sector conducts in managing its supply chain security through these industry-led standards, as well as other public-private initiatives with USG. Part of that due diligence is monitoring and complying with national security driven U.S. restrictive lists, such as the Department of Commerce Bureau of Industry

[5] *See eg.* Cybersecurity and Cyber Resilience Framework for the Securities and Exchange Board of India Regulated Entities, Circular No. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113, page 27 (Aug. 2024) (*available at https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html*)

and Security Office of Communications and Information Technology and Services determinations and FCC Covered List designations. Industry relies on these federal actions to provide insight into the national security threat landscape and to inform industry when certain suppliers present an undue risk and thus must be excluded from integration into U.S. critical infrastructure. TIA and our members support USG efforts to ensure that components and the network utilized by data centers come from trusted sources, and we understand that USG has an ongoing role to play in determining national security threats posed from non-trusted components of the ICT supply chain.

In this context, it is also worth highlighting industry and government action to mitigate threats posed by PRC vendors responsible for the manufacture of fiber optic cable. The Infrastructure Investment and Jobs Act, for example, included a prohibition on federal infrastructure funds being used on "fiber optic cable and optical transmission equipment manufactured in the People's Republic of China."[6] Additionally, the Fiber Broadband Association recently released "Measures to Define and Deploy Trusted Fiber," which looks to define a series of principles relating to quality and reliability, national security, corporate governance, and environmental sustainability.[7] Given the role that fiber plays in supporting data center growth, USG should approach potential action on this issue in a transparent way in dialogue with industry stakeholders.

Without clear U.S. government processes for these determinations and designations, and absent navigable guidance from the national security community for implementing them, the communications sector must undertake something of a "stabbing in the dark" approach regarding

[6] Pub. L. 117-58, § 60102(g)(1)(D)(ii)
[7] Fiber Broadband Association, *"Measures to Define and Deploy Trusted Fiber"* (Feb., 2024) https://fiberbroadband.org/wp-content/uploads/2024/03/FBA-Trusted-Fiber_-Feb-2023.pdf.

future untrusted suppliers and the specific national security risks they may carry. Where possible, our members urge USG to try to add certainty to this process in order to ensure security and resiliency in the ICT supply chain. Given the ongoing focus across government on companies that produce internet-connected and wireless components, the lack of transparency in the processes of how companies are added to these lists will result in disruptions, investment uncertainty, and other detrimental business impacts to communications sector companies over time. Thus, representing our members who are key components of the ICT sector, we recommend that the Department of Commerce engage with other agencies and industry to clarify processes and procedures and to reduce ambiguity regarding how this regime and other technology-based national security restrictive lists, such as the FCC's Covered List, will interact in the future. A more transparent process, coupled with broader use of available industry VCS that promote security, would better serve the ICT industry.

TIA industry programs support NTIA objectives

In addition to VCS standards like ANSI/TIA-942, TIA also maintains various industry programs and non-VCS process standards that are relevant to data centers and questions raised in the RFC.

- **Supply Chain Security Management System ("SCS 9001"):**[8] SCS 9001 is a Supply Chain Security Management System ("SCSMS"). It is a certifiable, process-based global standard with a specific focus on securing the supply chain of organizations operating in the ICT industry. As a fundamental requirement of securing its supply chain, an organization must demonstrate that it practices a proper level of security in protecting its operations, networks, devices, information, development process, and facilities, as examples. SCS 9001 provides assurance of the proper operational hygiene of network operators and their suppliers in delivering products and services of inherently higher security. It

[8] Telecommunications Industry Association, *Supply Chain Security*, https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/

encourages a culture of continuous improvement by requiring regular review to enhance security policies, procedures, and controls.

- **TL 9000 Quality Management System:** TL 9000 is a Quality Management System ("QMS") designed for the ICT industry. It is a certifiable, process-based global standard with a specific focus of building upon ISO 9001 in defining requirements covering the design, development, production, and operating lifetime of products and services used to implement and manage communications networks. In addition, TL 9000 provides an industry benchmarking program whereby specific measurements (key performance indicators) are identified to promote continuous improvement. Certified organizations participating in the program provide measurements which are anonymized and then used to create industry reports for suppliers and network operators to determine industry performance and trends across important quality metrics.
- **Broadband Nation:** TIA's Broadband Nation is a web portal that plays a crucial role in enabling a workforce to develop the necessary skills capable of contributing to the growth and innovation of the U.S. ICT infrastructure including data centers. The core of Broadband Nation is a collaboration between government, industry, and community stakeholders to invest in ICT infrastructure. It is a collective effort that will build the foundation for a workforce that is both digitally literate and technologically proficient. It matches workers to training and jobs that will enhance the digital infrastructure while enabling advanced ICT services such as broadband, 6G, AI, and IoT.

With these programs, TIA has a significant role to play in bolstering data center growth, resilience, and security. Certification and assessment programs associated with TIA and its standards should be leveraged by the USG and ICT organizations to enable data center growth, resilience, and security.

USG agencies and programs should provide financial support to individuals and organizations that operate and contribute to data center standardization efforts

Organizations involved in developing VCS do so at a cost. At least some time of their staff is dedicated to contributing their subject matter expertise to the committees that develop the standards. While standards are critical to organizations and countries, it is not always easy to see the benefits of the expense incurred in contributing to standards development because such development does not generate immediate and direct sales and revenue. TIA recommends that

USG provide financial support to individuals and organizations that operate and contribute to data center standardization efforts in order to encourage participation and enforce the importance of this contribution.

The National Institute of Standards and Technology ("NIST"), the National Telecommunications and Information Administration ("NTIA"), the National Science Foundation ("NSF"), and other agencies involved with supporting U.S. leadership and technology standards should include support for SDOs that develop standards relevant to data center design, build, operation, and growth under their broader remit.

Specific existing programs that may provide financial support for standardization efforts may include the NTIA's Public Wireless Supply Chain Innovation Fund, NIST's Capacity-Building Pilot Program for supporting SME participation in SDOs, and emerging lines of effort under the USG National Standards Strategy for Critical and Emerging Technology.

The Office of the United States Trade Representative should support policies that facilitate cross border data flows

One factor that drives U.S. data center demand is that U.S. data centers are able to serve global markets. This is in part because of international agreements supporting the crossborder transfer of data. The U.S. has historically been a leader in supporting the ability of enterprises, individuals, and others to transfer data across borders and has pushed back against countries like China that have instituted data localization requirements. This changed last year when the Office of the United States Trade Representative ("USTR") withdrew U.S. support for provisions in the WTO Ecommerce Moratorium that prohibit restrictions on crossborder data flows. This decision by a small group within USTR – without meaningful consultation of Congress, others agencies,

or other stakeholders – has drawn widespread criticism from both political parties,[9] from civil society groups like the ACLU and Freedom House,[10] and from the business community as a whole.[11]

The U.S. still has an opportunity to lead on digital trade and support U.S. data centers by promoting high-standard digital trade language in future trade negotiations. The U.S. Mexico Canada Agreement ("USMCA") provides a template for how parties might do this in Chapter 19 on Digital Trade, which reads in part:

> **Article 19.11: Cross-Border Transfer of Information by Electronic Means**
> 1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
> 2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure: (a) (b) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and does not impose restrictions on transfers of information greater than are necessary to achieve the objective.
>
> **Article 19.12: Location of Computing Facilities**
> No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.[12]

Promoting high-standard digital trade principles like these can help ensure that U.S. data centers can support digital exports around the world.

---

[9] See Ron Wyden, Mike Crapo, Thomas Carper, et al., *Letter to the President of the United States on WTO Digital Trade Negotiations* (Nov. 30, 2023) https://www.finance.senate.gov/imo/media/doc/20231130wydencrapolettertopotusonwtodigitaltradenegotiations.pdf.

[10] American Civil Liberties Union, Center for Democracy and Technology, Freedom House, et al., *Coalition Letter Urging Biden Administration to Protect Free and Open Internet*, ACLU (February 26, 2024) https://www.aclu.org/documents/coalition-letter-urging-biden-administration-to-protect-free-and-open-internet

[11] John Murphy, *Why Restoring America's Digital Trade Leadership Is Critical*, U.S. Chamber of Commerce (March 20, 2024), https://www.uschamber.com/international/trade-agreements/why-restoring-americas-digital-trade-leadership-is-critical.

[12] *U.S. Mexico Canada Agreement*, Can.-Mex.-U.S. (Jul. 1, 2020) https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between

Conclusion

TIA appreciates the opportunity to comment on this docket. We believe that broader adoption of VCS, such as ANSI/TIA-942, can help the government meet its data center objectives through appropriate reference and use. Additionally, other TIA industry programs in areas relating to quality management, supply chain security, and workforce development can support the healthy growth of the industry more broadly. We stand ready to work with NTIA and other government agencies as the need arises.

Signed:

Tom McGarry
Vice President of Standards

Patrick Lozada
Director, Global Policy

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1201 Wilson Boulevard, Floor 27
Arlington, VA 22209
(703) 907-7700

November 4, 2024