Before the
United States Department of Commerce
Washington, DC

In re Securing the Information and Communications Technology and Services Supply Chain	Docket No. 210113-0009 RIN 0605-AA51

COMMENTS OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

The Computer & Communications Industry Association ("CCIA") respectfully submits these comments in reply to the above-referenced proceeding.[1] CCIA represents large, medium, and small technology companies, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services.

I. Introduction

The Interim Final Rule ("the IFR") was drafted pursuant to Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, which states that the goal of this regulation is to "protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States."[2] While CCIA and its member companies share the goal of the Department of Commerce in securing Information and Communications Technology and Services ("ICTS"), we continue to have strong concerns about the IFR as it is currently

[1] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For nearly fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more, visit www.ccianet.org.

[2] 84 Fed. Reg. 22689 (May 17, 2019).

written. Companies and industry groups expressed wide-ranging concerns in comments responding to the initial Notice of Proposed Rulemaking ("NPRM"), and the Department addressed some of those concerns in the IFR.[3] However, the IFR does not adequately address industry's largest concerns. The scope of the IFR remains overly broad and lacks the transparency that companies need to conduct business. This lack of certainty could harm the U.S. technology sector, which would undermine the stated goals of Executive Order 13873 and the IFR. Furthermore, the IFR does not adequately take into consideration duplicative programs and regulations that already exist to review the national security implications of covered transactions. Although the IFR does take into consideration the Committee on Foreign Investment in the United States ("CFIUS") process, broader review of other existing programs is needed. Having duplicative review processes would further burden U.S. companies and would raise the risk of inconsistent decisions while negating the national security benefits of the IFR. For these reasons CCIA urges the Department of Commerce to reconsider the IFR and make changes to narrow the broad scope, provide increased transparency, and harmonize the IFR with existing processes.

II. The Broad Scope of the IFR Will Harm U.S. Industry Competitiveness.

The IFR notes that the ICTS supply chain "underpin[s] our economy," and that securing the ICTS supply chain must include protecting our "economic strength." Executive Order 13873 explains that the proposed regulation must balance national security concerns with "maintaining an open investment climate in information and communications technology, and in the United States economy more generally." The

[3] *See* Public Comments, *Securing the Information and Communications Technology and Services Supply Chain*, Department of Commerce, DOC-2019-0005; https://www.regulations.gov/document/DOC-2019-0005-0001/comment.

current IFR does not adequately balance these economic and business concerns. The scope of the rule is so broad and grants the Secretary of Commerce such wide-ranging authority that its application will likely harm U.S. business competitiveness, possibly undermining the rule's purpose of strengthening U.S. national security. In response to the initial NPRM, many commenters highlighted the very broad scope of the rule, and the lack of transparency. Although the updates in the IFR did address some of these concerns, the current scope of the rule is still overly broad. In response to these concerns, the Department attempted to clarify the definition of "ICTS transaction" as well as the scope of the covered ICTS transactions. Even under the clarified definition in the IFR, the Secretary of Commerce would have the authority to review almost any ICTS transaction with a named foreign adversary.[4] Furthermore, the IFR empowers the Secretary of Commerce to prohibit an ICTS transaction even after the transaction has occurred.

This broad authority would greatly increase uncertainty of doing business with U.S. companies. If virtually any transaction could be prohibited after the transaction is already complete, the risk of doing business with U.S. companies would naturally increase. As a result companies would need to incorporate the costs of this additional uncertainty into their transactions, which would lead to a less competitive U.S. technology sector. American companies playing a smaller role in the global ICTS supply chain would be counterproductive to the stated national security aims of the IFR. For these reasons, the scope of the IFR needs to be clarified and narrowed.

[4] *Securing the Information and Communications Technology and Services Supply Chain*, 86 Fed. Reg. 4912 (Jan. 19, 2021).

III. The IFR Fails to Consider Duplicative Government Programs and Review Processes.

In response to comments raising the concern that the NPRM would duplicate other existing U.S. programs, including CFIUS, the IFR clarified that the rule does not apply to ICTS transactions that CFIUS is actively reviewing or has reviewed, and that the Secretary is required to consult with other agency heads before making a final determination.[5] However, as the Department notes, CFIUS is not the only government authority that commenters cited. Other authorities that may overlap with the IFR include "authorities under various National Defense Authorization Acts; the Export Administration Regulations; the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, (i.e. Team Telecom); and other programs under the authority of the Federal Communications Commission, the Department of Homeland Security, and the Office of the Director of National Intelligence."[6] The Department of Commerce response says that the IFR is intended to "complement, not supplant, these existing regimes," but without coordinating with all the relevant existing regimes, the IFR is not complementing but rather duplicating processes.

A number of other government agencies have ongoing processes for review of the types of transactions covered under the IFR, and it is not sufficient to only harmonize with CFIUS review. For example, the Executive Branch's "Team Telecom" reviews foreign investments in telecommunications supply chains for national security issues

[5] 86 Fed. Reg. 4914 (Jan. 19, 2021).
[6] *Id.* at 4915.

prior to approval by the FCC.[7] The 2019 and 2020 National Defense Authorization Acts each contain provisions addressing national security risks in transactions with foreign adversaries.[8] The FCC has also recently restricted the use of certain telecommunications equipment from foreign adversaries in fifth generation wireless networks.[9] The IFR needs to be clear about how the new rules interact with these already existing processes. Subjecting ICTS transactions to multiple reviews is redundant and burdensome for companies, and would minimize the national security benefit of the new rule.

IV. Conclusion

Although CCIA and its members share the goal of ensuring security in the U.S. ICTS supply chain, we have serious concerns with the IFR as written. Despite the clarifications made in response to the NPRM comments, the scope of the rule is overly broad and leaves little certainty for industry. Furthermore, the IFR does not address duplicative regulations and review processes. In order to ensure that U.S. companies remain competitive while still ensuring the security of the U.S. ICTS supply chain, the Department of Commerce should review this rule and make significant changes to the current language.

---

[7] *See* The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector - Frequently Asked Questions, Dept. of Justice; https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector.

[8] *See Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (FAR Case 2018-017)*, 84 Fed. Reg. 40216 (August 13, 2019).

[9] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 85 Fed. Reg. 277 (Jan. 3, 2020).

March 22, 2021

Sincerely,

/s/ Vann Bentley
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Ave NW, Suite 300C
Washington, DC 20001
(202) 479-3771
vbentley@ccianet.org