July 21, 2025

Via ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
Washington, DC 20554

Re: Comments for GN Docket No. 25-166, *Protecting our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control*

The Computer & Communications Industry Association (CCIA)[1] is pleased to provide comment in this Federal Communications Commission (FCC or Commission) proceeding regarding "the national security, law enforcement, foreign policy, and trade policy risks that may be presented by foreign ownership and control of Commission licensees and authorization holders," in which the FCC "propose[s] to adopt requirements that would further our understanding of threats from foreign adversaries."[2]

I. INTRODUCTION

CCIA agrees that obtaining "increased transparency and visibility" is necessary as to entities that hold an interest in U.S. communications facilities or a Commission license to operate such facilities. NPRM ¶ 12. CCIA also agrees with the Commission's aim of "focusing on foreign *adversary* ownership or control, rather than foreign influence more broadly[.]" NPRM ¶ 1 (emphasis in original). As such, CCIA supports the NPRM's concentrating on how to craft disclosure and certification rules that will enable the Commission to discover "unacceptable risk" to the security of the U.S. communications network. NPRM ¶¶ 1, 3, 7.

II. CCIA SUPPORTS ADOPTION OF RULES THAT ENSURE THE SECURITY OF OUR NATION'S NETWORKS WITHOUT IMPOSING UNDUE BURDENS ON U.S. COMPANIES.

Bearing in mind the importance of requesting appropriate disclosures that enable the FCC and related agencies (*e.g.*, Team Telecom[3]) to verify that our nation's networks "are not subject to ownership, direction, or control that untrustworthy actors that pose a risk to national security," NPRM ¶ 10, the forthcoming rules should focus on entities that pose a demonstrable, appreciable risk to network security.

CCIA supports the Commission's proposed balance between obtaining "necessary information,

[1] CCIA is an international nonprofit membership organization representing companies in the computer, Internet, information technology, and telecommunications industries. Together, CCIA's members employ nearly half a million workers and generate approximately one quarter of a trillion dollars in annual revenue. CCIA promotes open markets, open systems, open networks, and full, fair, and open competition in the computer, telecommunications, and Internet industries. A complete list of CCIA members is available at http://www.ccianet.org/members.

[2] GN Docket No. 25-149, Notice of Proposed Rulemaking, FCC 25-28 ¶ 1 (rel. May 27, 2025), published at 90 Fed. Reg. 26244 (June 20, 2025) (the "NPRM").

[3] Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector, https://www.justice.gov/nsd/team-telecom (last visited July 20, 2025).

while not unduly burdening Regulatees without reportable Foreign Adversary Control." NPRM ¶ 48. A risk-based set of disclosure rules – requiring more information from entities with demonstrable and significant foreign adversary control – would strike this balance.

A. The Commission Should Exclude SDoC-Only Manufacturers from Its Proposed, Expanded Disclosure Rules.

The NPRM's proposed broad applicability to "authorization holders" (*e.g.*, ¶¶ 1, 12) might inadvertently include entities operating under the Supplier Declaration of Conformity (SDoC)[4] process, despite their differing risk profile compared to licensees that operate critical communications infrastructure. SDoC authorization holders, such as communications service providers that manufacture hardware in-house for internal use, do not pose the same systemic risk as operators of public networks and direct-connectivity infrastructure. CCIA suggests that the Commission should explicitly clarify that entities obtaining authorization solely under the SDoC process are not subject to mandatory certification or reporting unless the equipment is designated as high-risk. This approach is consistent with other federal risk-based models that focus regulatory oversight on national security-sensitive equipment.

Cloud service providers already adhere to several federal frameworks established to safeguard national security. These frameworks include the Secure Equipment Act of 2021, the vetting of internal ownership and supply chain management, CFIUS oversight of investments and acquisitions, and adherence to procurement standards that comport with NIST SP 800-161. Imposing duplicative reporting or certification obligations on entities that already operate within these frameworks would introduce regulatory inefficiencies without any incremental national security benefit.

To minimize the compliance burden while preserving FCC oversight authority, CCIA recommends a safe harbor self-certification for entities without known foreign adversary control. Such entities could file a one-time attestation, providing documentary evidence upon request. In addition, the Commission should establish a presumption of compliance for manufacturers not producing radiofrequency or other national-security-relevant equipment. This targeted approach would align regulatory burden with actual risk exposure.

B. The Commission Should Limit the Proposed Certification Requirement to Regulated Entities That Have Reportable Foreign Adversary Control.

CCIA agrees that the Commission should limit certification requirements to entities with actual or reportable foreign adversary ownership or control. NPRM ¶ 48. This targeted approach appropriately prioritizes national security concerns while avoiding unnecessary filings from entities with no relevant foreign ties. CCIA supports adoption of the 5% threshold for "direct or indirect equity and/or voting interest holders" for identifying entities with reportable foreign adversary control. NPRM ¶ 49.

Further, CCIA recommends that the FCC align its control thresholds with those used by other national security bodies, such as the Committee on Foreign Investment in the United States (CFIUS) and Team Telecom. Such alignment would promote regulatory clarity, reduce

[4] *See generally* Nat'l Institute of Standards and Technology, *The Use of Supplier's Declaration of Conformity*, www.nist.gov/system/files/documents/standardsgov/Sdoc.pdf (last visited July 20, 2025).

compliance costs for low-risk entities, and allow the Commission to concentrate its resources on high-risk ownership structures that genuinely run the risk of compromising U.S. communications infrastructure.

C. The Commission Should Require Enhanced Disclosures for High-Risk Entities.

In keeping with the risk-based approach suggested above, the Commission should impose enhanced disclosure obligations for entities that pose significant risk to U.S. communications networks. For entities with identified foreign adversary ties, the Commission could require enhanced disclosures of information such as interactions with foreign governments and political parties and detailed presentation of ownership structures that involve sensitive sectors. In line with the Commission's requiring enhanced transparency concerning critical components of these entities' public networks and the devices that leverage them, it should also specifically consider the potential presence of on-device software controlled by foreign adversaries that could exploit network vulnerabilities. These requirements should be expressly limited to high-risk profiles and crafted to avoid overly broad or vague interpretations.

D. The Commission Should Avoid Duplicative Disclosure Obligations for Entities Subject to Team Telecom Mitigation Agreements.

As stated above, CCIA supports adoption of rules that ensure transparency and visibility without imposing unduly burdensome requirements. Duplicative disclosure obligations are invariably unduly burdensome to both filers and to government agencies. Therefore, CCIA urges the Commission not to impose multiple layers of disclosure requirements on licensees that already are subject to Team Telecom mitigation agreements. Instead, the FCC should coordinate with Team Telecom and relevant agencies to share licensee information about their ownership and control. If a licensee has satisfied the disclosure requirements for one agency of jurisdiction, the FCC has no need to demand duplicative filings from that licensee. Not only would this policy protect licensees, it would also help the Commission streamline its oversight while protecting sensitive information already reviewed under national security protocols.

E. The Commission Should Establish a System for Interagency Data Sharing.

In addition to the disclosure obligations proposed in the NPRM, CCIA supports the establishment of an interagency information-sharing framework that enables secure, confidential transmission of ownership and compliance data between the FCC and relevant agencies. Were a protocol established for routinized interagency data sharing, Regulatees would avoid the needless burden of making multiple, identical filings of the same information. This protocol would serve the risk v. burden balance that the Commission seeks to strike. NPRM ¶ 52.

F. The Commission Should Allow Sufficient Time for Compliance With Reporting Requirements.

The Commission's proposed 60-day reporting window and 30-day lookback period (NPRM ¶ 63) do not provide sufficient time for Regulatees—especially SDoC authorization holders, who may have many authorizations and no existing foreign ownership reporting obligations—to meet the new certification requirements. Ownership information can take time to collect and delays from interest holders are common. Premature enforcement could disrupt supply chains and cloud services if suppliers lose authorizations before they can comply. CCIA recommends extending

the reporting window to 120 days, allowing certifications based on ownership information as of 30 days before filing, offering extensions for good-faith efforts to meet the deadline, and providing 60 days to cure any deficiencies. The Commission should also consider a one-time collection from existing Regulatees before applying these rules to all applicants and allowing Regulatees to report changes within 30 days rather than certifying annually.

* * * *

CCIA appreciates the opportunity to participate in this proceeding and is available to provide any additional information that might be helpful to the Commission.

Sincerely,

Stephanie Joyce
Chief of Staff and Senior Vice President
CCIA