The Communications and Technology Transparency Act of 2026
Section-by-Section

The **Communications and Technology Transparency Act of 2026** is bipartisan legislation that seeks to update and improve the Secure and Trusted Communications Networks (Secure and Trusted) Act of 2019. This Act streamlines the process for barring malicious technology and equipment from foreign adversaries from coming into the United States and clarifies the method for determining what is considered malicious technology or equipment. This Act will improve the consistency and transparency around the Federal Communications Commission's (FCC) covered list, ensuring that it targets foreign adversaries and is used as Congress intended to safeguard our national security. The following section-by-section outlines the objectives of the Act.

Sec. 2. Information and Communication Technology or Services

- Section 2 expands the "communications equipment or service" language in the Secure and Trusted Act of 2019 to "information and communications technology or service" as defined in the Department of Commerce's regulations.
- This update broadens the types of technologies the FCC must add to its covered list and creates better alignment between the FCC's national security work and the Department of Commerce's work.

Sec. 3. Reliance on Certain Determinations

- Section 3 streamlines the national security determinations that the FCC must rely on to place information and communications technology or services on its covered list.
- This update better aligns the FCC's national security efforts with Congress's work and the Department of Commerce's established process for evaluating the national security risks of information and communications technology or services.

Sec. 4. Updating of List

- The Secure and Trusted Act directs the FCC to periodically update and monitor its covered list. Section 4 would update this directive to ensure that FCC updates the covered list at least every six months, as well as provides a transparent process for monitoring and removing any information and communications technology or services from the list.
- These "good government" solutions will offer the consistent assessment and placement of rogue information and communications technology or services on the FCC's covered list.

Sec. 5. Matters Related to Additions To and Removal from List

- Section 5 would require the FCC to only place those information and communications technologies or services on its covered list that are produced or provided by an entity that is controlled by a "foreign adversary." Consistent with federal law, a "foreign adversary" means the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of North Korea.

- Section 5 also requires the FCC to report to Congress at least seven days in advance before placing any information and communications technology or service on its covered list.
- Section 5 further allows Congress to use the Congressional Review Act on decisions to add or remove a class or category of information and communications technologies or services that does not reference a particular entity.
- Collectively, these new requirements will ensure that the FCC's covered list targets foreign adversaries and is used as Congress intended to safeguard our national security.

Sec. 6. Transmission of Notices of Risk

- Section 6 establishes a formal requirement for the FCC to notify the Secretary of Commerce within 60 days if it receives notice that an information and communications technology or service poses an unacceptable risk to national security. The Secretary will then review this notice consistent with its regulations.

Sec. 7. Consultation and Coordination

- Section 7 establishes the requirement that FCC and the Secretary of Commerce must meet every 90 days to consult and coordinate about the covered list and submit an annual report to Congress on these coordination efforts. The FCC and the Secretary must also provide the relevant national security agencies with the opportunity to participate in these meetings.
- The requirements in Section 6 and Section 7 ensure that the FCC and the Department of Commerce remain in close coordination with each other and our national security agencies to assess and remove any threats to our country's technology and telecommunications equipment and networks.

Sec. 8. Certain Authorizations, Licenses, and Other Grants of Authority Prohibited

- Section 8 builds on the House's efforts in the Secure Space Act of 2025 by establishing that the FCC may not grant any entity on its covered list or its affiliates (as defined in the Communications Act) any FCC authorization, license, or other grant of authority.
- This requirement will cut off another path for our foreign adversaries to gain access to our tech and telecom equipment and networks.

Sec. 9. Equipment Authorizations

- Section 9 clarifies that the FCC is not required to retroactively review or revoke any equipment authorization that was granted before the relevant equipment was placed on its covered list.
- This requirement offers stability to American consumers and companies so that they do not face a sudden disruption by the placement of certain technology or equipment on the FCC's covered list.