

Summary of “Banned in D.C.: Examining Government Approaches to Foreign Technology Threats”

Since 2018, federal law and policymakers have enacted several measures to restrict the procurement and use of foreign information and communications technology and services (ICTS) that pose national security risks. These include:

- Section 889 (Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment) of the 2019 National Defense Authorization Act;
- Title 2 (Federal Acquisition Supply Chain Security Act of 2018) of the SECURE Technology Act;
- The U.S. Department of Commerce’s rule on Securing the ICTS Supply Chain; and,
- The Secure and Trusted Communication Networks Act of 2019.

This report provides an overview of these federal measures as well as several state procurement prohibitions and offers recommendations for building a more cohesive approach to supply chain security nationwide.

While federal agencies have started to address foreign technology threats, state and local governments have been slow to act. Just five states—Florida, Georgia, Louisiana, Texas, and Vermont—have attempted to restrict the procurement of untrustworthy foreign ICTS, with limited effectiveness. A CSET analysis of procurement records found that in recent years at least 1,681 state and local governments purchased federally banned ICTS.

Keeping untrustworthy foreign technology out of U.S. networks requires a more coordinated approach to supply chain security spearheaded by the federal government. Federal policymakers must develop and enact adaptable and effective procurement prohibitions. Further, Congress should provide the Commerce Department with the resources necessary to implement the ICTS rule, and the Federal Communications Commission should block authorizations of equipment produced by entities on its covered list.

State and local governments should not be expected to independently grapple with foreign technology threats; however, they **can protect their digital infrastructures by adhering to federal guidance on foreign ICTS procurement—including following mandatory restrictions and potentially aligning procurement practices with federal bans.** Federal policymakers can further empower state and local governments by publishing a master list of procurement prohibitions, strengthening existing information sharing channels, and increasing funding for rip and replace programs.

For more information:

- Download the report: <https://cset.georgetown.edu/publication/banned-in-d-c>
- Contact us: Jack Corrigan (jack.corrigan@georgetown.edu).