

How FCC Covered List Blitz Is Sidelining Commerce Dept.

WRITTEN BY

Peter E. Jeydel

This article was originally published on [Law360](#) and is republished here with permission as it originally appeared on August 21, 2026.

Since the start of the second Trump administration, the [Federal Communications Commission](#) has been on a tear, taking unprecedented action by adding a wide array of foreign-produced technologies to its Covered List, essentially cutting them off from the U.S. market absent specific approvals or exemptions. At the same time, the [U.S. Department of Commerce](#)'s Office of Information and Communications Technology and Services, or OICTS, has not imposed any new restrictions, despite years of work in many of the same areas.

For example, in July alone, the FCC [imposed](#) industry-changing regulations on foreign-produced power inverters and advanced robotic devices, both of which are sectors in which the OICTS had been considering taking — but never moved forward with — its own regulatory actions.

This trend raises serious questions about the purpose and future of the OICTS, and how the U.S. government will go forward in imposing national security regulation on domestic applications of adversary-linked technologies. Equally important are questions about the durability of the FCC's apparent lead in this regulatory effort, particularly as it appears to stretch its authorities in untested ways.

BACKGROUND

The OICTS traces its origins to President Donald Trump's May 2019 Executive Order No.13873, setting out the broad information and communications technology and services supply chain review authority that the OICTS still relies on today.

The proposed rule establishing the detailed ICTS regulatory framework followed shortly thereafter, in November 2019. Among the final acts of the first Trump administration was the Jan. 19, 2021, publication of the interim final rule that put the ICTS regulatory structure formally in place.

The momentum behind the OICTS accelerated under the Biden administration. The office was formally established in March 2022 within the Commerce Department's [Bureau of Industry and Security](#).

The OICTS then had a banner couple of years. In June 2024, it announced a broad prohibition on products tied to [Kaspersky Lab](#), a Russia-based antivirus software and cybersecurity company that had been embedded in U.S.

systems for many years. Then, in September 2024, the OICTS shook up the auto industry by issuing a proposed rule effectively banning connected vehicles and certain related technologies tied to China or Russia. In December 2024, it published its final rule for the overarching ICTS regulatory framework.

The OICTS also made a big splash in 2024 with its technology prioritization table listing 16 broad technology areas it was looking to regulate, including energy generation and storage, autonomous systems and robotics, advanced cloud services, and others. Coming along with the industry-changing connected vehicle rule, also published in 2024, this was a strong indication that OICTS was poised to dramatically reshape how foreign technology could be used in the U.S.

The Biden administration, in its waning days, took a few final actions under the auspices of the OICTS, publishing a notice in the fall of 2024 indicating an intent to regulate under the ICTS authority on cloud computing and data center products and services, and another in January 2025 for [unmanned aerial systems](#), or UAS. It finalized the connected vehicle rule in January 2025 as well.

All of this left no doubt in the minds of many practitioners that the OICTS was a force to be reckoned with, and that its impact on industry was just beginning to be felt as it continued to ramp up.

Across town from the Commerce Department, things in this area were much quieter at the FCC. The FCC's Covered List campaign was launched under the Biden administration in 2021, though it was based on statutory authority dating from the first Trump administration. But the Biden FCC was relatively slow and cautious in its Covered List designations, initially tackling prominent Chinese technology and telecommunications firms with targeted restrictions.

The FCC in 2024 played a role in the Kaspersky action, alongside the sweeping restriction imposed by the OICTS. All signs at this time were pointing at the FCC continuing to play a relatively narrow part in the regulation of adversary technologies in the domestic market, with the OICTS leading the charge by aggressively regulating major dependencies.

The second Trump administration, even while discarding and disrupting countless Biden-era regulatory programs in its early days, expressed clear support for the OICTS — again, originally a creature of the first Trump administration. For example, the America First Trade Policy memorandum, issued Jan. 20, 2025, directed the secretary of commerce to “consider whether controls on ICTS transactions should be expanded to account for additional connected products.”

But soon thereafter a period of eerie calm set in at the BIS, with the OICTS making no significant new announcements under the second Trump administration. In fact, the administration halted the UAS rulemaking process, among the first concrete signs that the current Trump White House may have serious questions about the agenda of the OICTS.

At the same time, however, the connected vehicle rule's implementation has been moving forward largely as expected, and there has been a low hum of activity from the OICTS in connection with that rule, providing clear proof of life within the office.

THE FCC'S COVERED LIST BLITZ

Now we may be experiencing a role reversal, but one that has sowed real doubts in the minds of many industry participants about the sustainability of the FCC's newfound zeal. Despite its historically modest role in this area, it is the FCC that has taken the reins of domestic-technology regulation for national security purposes in 2025 and so far in 2026.

The commission has moved forward on numerous fronts simultaneously, with unprecedented scope and speed, and often venturing beyond what many view as the limits of its statutory authority. The FCC's main vehicle for carrying out this national security agenda has been the Covered List.

The last few months have seen the FCC pushing out remarkably broad and highly disruptive new restrictions under the Covered List, one after the next. A significant new trend is the FCC naming categories of equipment, rather than just individual companies, greatly expanding the reach of these restrictions.

Recently announced Covered List entries span the following broad sectors:

- Foreign-produced UAS/drones and critical components (December 2025);
- Foreign-produced routers (March 2026);
- Foreign-produced power inverters (July 2026); and
- Foreign-produced advanced robotic devices (July 2026).

Notably, these new restrictions can cover devices with no connection at all to any adversary country, a much wider sweep than the FCC had previously attempted, raising important questions about both the policy rationale and the legal authority supporting the breadth of these actions. The FCC even added a U.S. company, DigitalSystem Technology, to the Covered List in July, alleging various links to China — ownership, partnerships, etc.

Furthermore, the FCC has continued expanding the impact of a Covered List designation. For example, it recently advanced a rule to bar U.S. telecom carriers from interconnecting with designated entities, and to prohibit certain of them from operating data centers and other infrastructure in the U.S. Many of the areas targeted by the FCC are those that the OICTS had previously attempted to regulate — e.g., UAS and data centers.

This is not how many observers had expected this to play out. The FCC has relatively narrow authority in this realm. FCC regulations generally prohibit marketing, operation, etc. of radio frequency devices without valid FCC equipment authorization, and prohibit such authorization for devices falling within a Covered List entry.

So being on the Covered List essentially bans the device from the U.S. market going forward, based on its radio frequency emissions. It is really the near-ubiquity of radio frequency emissions in modern devices that has made the FCC's view of its own authority so wide-ranging. Moreover, the FCC is technically a mere implementer in this area, empowered essentially only to promulgate and administer regulations proposed by other national security agencies. Still, a number of actions and statements by FCC officials in recent months indicate that they view themselves — and want to be viewed — as being in the driver's seat to a large degree.

The OICTS, on the other hand, has incredibly broad authority to regulate “any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service ... designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction

of foreign adversaries.” The OICTS was created recently, and specifically, for the purpose of leading this type of domestic technology national security regulation. It was started under the first Trump administration, developed under the Biden administration, and then appeared to have the support of the second Trump administration at the outset.

So it is important to question why the OICTS has been overshadowed by the FCC since early 2025 in the very domain that the OICTS was created to regulate. There has been no shortage of reporting about apparent turmoil within the OICTS’s parent agency, the BIS, as well as the recent departures of OICTS leadership along with much of the BIS’ career leadership and senior staff, and the considerable friction between BIS’ political leadership and certain key members of Congress.[1]

There has been speculation among practitioners that the deliberative process within the OICTS was not delivering results quickly enough, as that office tried to consider the implications of its actions with care, and craft them as thoughtfully and narrowly as possible. This could be viewed as a contrast to the move-fast-and-break-things approach that the FCC seems to have favored recently — designating wide swaths of technology, and then leaving it to individual companies to seek variances from the broad restrictions in real time as they continue to try to operate their businesses with these dependencies.

Whatever the reasons may be for the apparent ascendancy of the FCC in this area in the past few months, if this recent trend continues, there will be serious questions about the future of the OICTS and what role it will have in protecting Americans against national security threats presented by adversary technologies.

It is not hard to imagine that a combination of industry pushback and successful litigation could begin to defang the FCC. This could lead the pendulum to swing back to the OICTS, with its more deliberative approach and broad authority specifically targeting national security risks stemming from adversary technologies.

Indeed, as laid out in remarkable detail in a report this month by the U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party — “Stranger Pings: Chinese Telecom Companies Infiltrate U.S. Infrastructure” — the threats identified “cannot be stopped by FCC rulemaking alone,” because “there remains a significant legislative gap.”

It is not hard to picture the wry smiles of the House staffers who wrote in that report that the FCC’s recent rulemakings have been exploring “the outer limits of its authority.” Once the BIS at the Commerce Department is able to get through its current rough patch, it is fair to expect a new thrust of action under the ICTS framework, targeting adversary technologies that the FCC cannot effectively regulate.

[1] <https://www.politico.com/news/2026/07/08/trump-ai-tech-chips-exports-00989167>; <https://www.reuters.com/world/asia-pacific/trump-administration-pushes-out-official-whose-unit-banned-chinese-vehicles-2026-01-23/>.

RELATED INDUSTRIES + PRACTICES

- [Sanctions + Trade Controls](#)