Skadden

Cybersecurity and Data Privacy Update

April 11, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the next page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

FCC Council on National Security Launches Investigation of Businesses Linked to the Chinese Communist Party

In its first major initiative, on March 21, 2025, the Federal Communications Commission's (FCC's) newly formed Council on National Security (Council) launched an investigation into the "ongoing U.S. operations" of businesses aligned with the Chinese Communist Party (CCP) that appear on the FCC's Covered List. Despite prior regulatory actions — including the revocation of FCC authorizations — FCC Chairman Brendan Carr stated there is reason to believe some of these entities continue to operate in the U.S. through unregulated or indirect channels.

The investigation, which involves letters of inquiry and at least one subpoena, is focused on gathering detailed information about these companies' activities and identifying any third parties enabling them. The FCC has pledged to act quickly to close regulatory loopholes that may allow foreign adversary-backed businesses to circumvent national security safeguards.

The FCC announced the formation of the Council on March 13, 2025. Chairman Carr stated then that the Council will utilize the full breadth of the commission's "regulatory, investigatory, and enforcement authorities" to bolster U.S. national security and address foreign threats, with particular focus on adversarial activity linked to the People's Republic of China (PRC) and the CCP.

He emphasized the "persistent and constant threat from foreign adversaries, particularly the CCP," and highlighted the importance of the FCC's vigilance in protecting American networks, devices and the broader technology ecosystem.

The Council will focus on three objectives:

- Reducing the technology and telecommunications sectors' reliance on foreign adversaries for trade and supply chain needs.
- Mitigating vulnerabilities to "cyberattacks, espionage, and surveillance by foreign adversaries."
- Ensuring that the U.S. maintains a competitive edge over China in critical technologies, including "5G and 6G, AI, satellites and space, quantum computing, robotics and autonomous systems, and the Internet of Things."

The Council will include representatives from eight different bureaus and offices within the FCC, promoting "cross-agency collaboration and information sharing." This structure is designed to enhance the FCC's ability to implement a comprehensive national security agenda and to facilitate engagement with national security partners across the executive branch and Congress.

FCC Council on National Security Launches Investigation of Businesses Linked to the Chinese Communist Party

Update on FCC's Cybersecurity Rules

In December 2024, under the leadership of then-Chair Jessica Rosenworcel, the FCC proposed new cybersecurity rules aimed at strengthening the defenses of telecommunications networks. These proposals were largely in response to significant cyber espionage campaigns, notably the "Salt Typhoon" attack, attributed to state-sponsored actors from the PRC, which compromised multiple U.S. telecommunications providers.

The measures included:

- Declaratory Ruling: Clarifying that telecommunications carriers are legally obligated under Section 105 of the Communications Assistance for Law Enforcement Act (CALEA) to secure their networks from unlawful access or interception of communications.
- Notice of Proposed Rulemaking (NPRM): Requiring communications service providers to develop, implement, and annually certify cybersecurity and supply chain risk management plans.

On January 16, 2025, the FCC enacted the Declaratory Ruling, making it immediately effective. The NPRM is currently in the public comment phase, with the future of the regulatory measures contingent on the new FCC leadership under Chairman Carr.

Conclusion

The establishment of the Council reflects a growing emphasis on safeguarding the telecommunications and technology sectors from foreign cyber and other national security threats. Companies operating in these industries should anticipate increased regulatory scrutiny, particularly concerning supply chain security, network integrity and compliance with emerging national security-related cybersecurity mandates.

The cybersecurity rules proposed in the final days of the Biden administration remain under review, with the Declaratory Ruling now in effect and the NPRM still in the public comment phase. The direction of these regulatory measures under Chairman Carr remains to be seen, but companies should expect an intensified focus on limiting foreign access to U.S. communications infrastructure and strengthening network security requirements.

As the FCC expands its focus on national security issues, companies should proactively assess their cybersecurity programs, vendor relationships, software and hardware supply chains, and risk management strategies to align with anticipated regulatory changes. Given the potential for heightened scrutiny, companies should be particularly vigilant if their software or hardware is being developed in jurisdictions such as China or Russia, as these activities may be subject to increased examination by regulators. Engaging with the FCC and other national security agencies will be critical in navigating this shifting landscape. We will continue to monitor and provide updates as policies and enforcement priorities evolve.

Contacts

Brian J. Egan
Partner / Washington, D.C.
202.371.7270
brian.egan@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Melissa Muse
Associate / Washington, D.C.
202.371.7022
melissa.muse@skadden.com

Jake O. Seaboch
Associate / New York
212.735.2038
jake.seaboch@skadden.com