Overview

Safeguarding America’s communications networks from national security threats is more critical than ever. That’s why Chairman Pai has circulated a two-part proposal, which the FCC will vote on at its November 19 meeting, to protect U.S. communications networks from national security threats.

First, a draft Report and Order would prohibit companies from using money from the FCC’s $8.5 billion Universal Service Fund (USF) to purchase equipment or services from any company that poses a national security threat. The draft Report and Order would initially designate two Chinese companies—Huawei and ZTE Corporation—as companies that pose a national security risk and would establish a process for designating additional covered companies in the future.

Second, a draft Further Notice of Proposed Rulemaking and draft Information Collection Order would propose to remove and replace equipment produced by covered companies from USF-funded communications networks. Chairman Pai’s plan calls for:

- An assessment to find out how much Huawei and ZTE equipment is in these networks and the costs to remove and replace it; and
- Financial assistance to carriers to help them transition to more trusted suppliers.

Report and Order – Prohibiting the Use of USF Funds to Purchase Equipment or Services from Suppliers that Pose a National Security Threat

Chairman Pai’s draft Report and Order would adopt a rule that prohibits the use of USF funds to purchase or obtain any equipment or services produced or provided by a covered company—i.e., one that poses a national security threat to the integrity of communications networks or the communications supply chain.

In the draft Report and Order, the FCC would initially designate Huawei and ZTE as covered companies for purposes of this rule, and it would establish a process for designating additional covered companies in the future. Both companies’ ties to the Chinese government and military apparatus—together with Chinese laws requiring that such companies assist the Chinese government with intelligence activities—pose a threat to the security of U.S. communications networks and the communications supply chain.

Because the rule is prospective, it would not itself prohibit the use of existing equipment or services already deployed or in use. USF recipients may continue to use equipment or services produced or provided by covered companies obtained prior to the issuance of the rule, but may not use USF funds to maintain, improve, modify, or otherwise support such equipment or services in any way.

Further Notice of Proposed Rulemaking – Removal and Replacement

In the accompanying draft Further Notice of Proposed Rulemaking, the FCC would propose additional actions to address national security threats to USF-funded networks. Specifically, it would propose to require carriers receiving USF funds, known as eligible telecommunications carriers, to remove existing equipment from covered companies, starting with Huawei and ZTE, from their networks. To mitigate the impact on affected entities, and in particular small, rural carriers, the FCC would propose to establish a reimbursement program to help offset the transition cost.
Information Collection Order

To aid the design of a removal and replacement program, the draft Information Collection Order would seek information from eligible telecommunications carriers on their use of equipment from Huawei and ZTE as well as the potential costs associated with the removal and replacement of such equipment.

Additional Resources

A bipartisan group of 18 Senators and Representatives wrote to the FCC regarding their concern about Chinese telecommunications equipment: https://docs.fcc.gov/public/attachments/DOC-349859A2.pdf.

- “Both the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence have long been concerned about Chinese espionage in general, and Huawei’s role in that espionage in particular.”


- “Given the national security risks, we believe it’s time for more concerted federal action. Among other things, that means making sure that our government doesn’t make the problem worse by spending the American people’s money on products and services from any company that poses a national security threat to our communications networks.”