

U.S. Charges Huawei with Theft of Trade Secrets; Risks for Carriers Using Huawei Equipment Increase

January 30, 2019

In a move certain to inflame the ongoing trade dispute between the United States and China, Justice Department officials [announced criminal charges](#) against Chinese telecommunications equipment manufacturer Huawei, several of its affiliates, and its chief financial officer for alleged theft of trade secrets from U.S. telecommunications providers, bank fraud, obstruction of justice, and other violations. The [two indictments](#) issued on January 28, 2019, represent just the latest pushback against foreign telecommunications interests by U.S. officials, citing national security concerns and unfair trade practice claims. The FCC already [proposed rule changes](#) last year that would prohibit the use of Universal Service Fund support to purchase equipment or services from foreign companies deemed national security threats, primarily targeting companies from China and Russia. Congress also recently passed [legislation](#) prohibiting federal agencies and those working with them from using components provided by Huawei and other Chinese manufacturers. With the Trump Administration reportedly poised to issue an executive order effectively barring American companies from using Chinese-origin equipment in critical telecommunications networks, domestic service providers should keep a close eye on their supply chain security and potential liability when working with foreign entities. A criminal conviction on these charges could lead to broader restrictions on trade in U.S. export-controlled products with the company. Given the presence of encryption in telecom equipment, export controls on such products are relatively widespread

The Justice Department accused Huawei of stealing trade secrets and materials used to test mobile phones from a major U.S. telecommunications carrier. The criminal charges stem from an earlier civil suit brought by the U.S. carrier, in which Huawei was found guilty and ordered to pay compensation. Prosecutors alleged that Huawei encouraged corporate espionage, offering bonuses to employees who succeeded in stealing confidential information from U.S. competitors. In addition, Huawei, several of its affiliates, and its chief financial officer were charged with bank fraud for purportedly misleading U.S. banks into clearing transactions with Iran in violation of international sanctions. Officials also claimed that Huawei obstructed justice by allegedly moving witnesses outside of U.S. jurisdiction, destroying evidence, and lying to Congress about its association with Iranian business interests.

While the U.S. governments' investigation into Huawei is ongoing, the indictments show the national security and trade risks inherent in working with foreign telecommunications interests. Federal officials continue to advocate action to impede or outright block the use of foreign-made equipment in critical telecommunications networks, particularly those forming the backbone of next-generation 5G wireless technologies. However, some smaller U.S. carriers have raised concerns with the pushback, pointing to potential cost increases due to restricted access to foreign components and resulting detrimental effects on broadband deployment in rural areas. As a result, it remains to be

seen how U.S. policymakers plan to balance national security and trade objectives with broadband deployment and telecommunications innovation goals. For those using or considering using Huawei equipment, careful monitoring of the open FCC proceeding is advisable.