Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

New FCC Rules Ban Authorizations for Equipment Posing National Security Risks

January 11, 2023

On November 25, 2022, the Federal Communications Commission (FCC) released new rules restricting equipment that poses national security risks from being imported to or sold in the United States. Under the new rules, the FCC will not issue new authorizations for telecommunications equipment produced by Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE), the two largest telecommunications equipment manufacturers in the People's Republic of China (PRC). The FCC also will not authorize equipment produced by three PRC-based surveillance camera manufacturers—Hytera Communications (Hytera), Hangzhou Hikvision Digital Technology (Hikvision), and Dahua Technology (Dahua)—until the FCC approves these entities' plans to ensure that their equipment is not marketed or sold for public safety purposes, government facilities, critical infrastructure, or other national security purposes. The FCC did not, however, revoke any of its *prior* authorizations for these companies' equipment, although it sought comments on whether it should do so in the future.

These new rules are the latest action in the federal government's broader effort to secure U.S. communications networks and prohibit the use of equipment that could give a foreign adversary the ability to exploit those networks. This Sidebar starts by providing a brief background on past steps taken by the federal government, particularly the FCC, to protect communications networks from national security risk. The Sidebar then reviews the FCC's role in authorizing equipment and explains how the new rules fit into that authorization process. The Sidebar then discusses potential legal challenges to the new rules and concludes with some considerations for Congress.

Prior Efforts to Protect U.S. Communications Networks from Foreign Adversaries

As explained in another CRS Report, the federal government has taken several steps in recent years to secure U.S. communications networks from potential exploitation by foreign adversaries. For example, in Section 889 of the National Defense Authorization Act for Fiscal Year 2019 (FY2019 NDAA), Congress restricted Executive Branch agencies from procuring systems that use Huawei, ZTE, Hytera, Hikvision, or Dahua equipment or services and from contracting with companies that use their equipment or services. The Department of Commerce has also set up a process for reviewing, and potentially

Congressional Research Service
https://crsreports.congress.gov
LSB10895

prohibiting, transactions that impact the information and telecommunications technology and services (ICTS) supply chain and raise national security concerns, as discussed in a CRS In Focus.

The FCC has also acted to address national security risk in communications networks. First, the FCC prohibited several PRC telecommunications carriers from providing telecommunications services between the United States and abroad. Under Section 214 of the Communications Act, telecommunications carriers must obtain an authorization from the FCC before building, operating, or extending a communications line between the United States and a foreign point. Applications to the FCC for these international communications lines are reviewed for national security concerns by an interagency Executive Branch committee (Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, formerly known as Team Telecom), who may recommend to the FCC that the application be denied or may recommend that existing authorizations be revoked. In recent years, the FCC has revoked or denied international Section 214 authorizations for several PRC telecommunications companies—including China Mobile, China Telecom, China Unicom, and Pacific Networks—based on the executive branch agencies' assessment that the PRC government controls these firms and related concerns about government influence on these companies. China Telecom challenged the FCC's revocation decision in federal court, but the U.S. Court of Appeals for the D.C. Circuit rejected the challenge in an opinion issued under seal (i.e., unavailable to the public).

The FCC has also sought to remove equipment raising national security concerns from U.S. telecommunications infrastructure through its Universal Service Fund (USF) restrictions and reimbursement program. The USF subsidizes voice and broadband internet service in rural and high-cost areas. As discussed further in a CRS Report, the FCC has restricted telecommunications carriers receiving USF funds from using equipment or services that appear on a "Covered List" published by the FCC. The Covered List currently includes equipment and services provided by the PRC-based companies Huawei, ZTE, Hytera, Hikvision, Dahua, China Mobile, China Telecom, China Unicom, and Pacific Networks. It also includes information security products and services provided by the Russian cybersecurity company Kaspersky Lab. While the FCC first established the USF restrictions on its own initiative, in March 2020 Congress passed the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), which prohibits the use of FCC subsidies for the purchase, lease, or maintenance of equipment or services appearing on the Covered List. The Secure Networks Act also provides additional direction for the FCC's maintenance of the Covered List, and it creates a program to reimburse carriers for the costs of replacing "covered equipment" in their networks, as detailed in a CRS Insight.

The FCC's Equipment Authorization Authority

Most recently, the FCC has used its equipment authorization authority to restrict electronic devices raising national security concerns. The Communications Act authorizes the FCC to adopt regulations, consistent with the "public interest," that govern the "interference potential" of devices capable of emitting radio frequency (RF) energy. Under this authority, the FCC has adopted rules requiring RF devices to be authorized by the FCC before being imported or marketed in the United States. The FCC has explained that "[a]lmost all electronic-electrical products" are subject to this authorization requirement.

The authorization process follows two paths, depending on the nature of the device. The first path is certification, which applies to equipment with the greatest potential to cause harmful interference to radio services. This category mainly includes "intentional radiators" designed to emit RF energy (such as cell phones, Bluetooth radio devices, and wireless garage door openers). Under the certification process, authorization applications are reviewed and approved by a Telecommunications Certification Body, which evaluates the device's document and test data to see if it complies with Commission rules. The second path is the Supplier's Declaration of Conformity (SDoC) process, which applies to electronic devices that have no radio transmitters and pose less risk for harmful interference (such as computer peripherals,

microwave ovens, and LED lightbulbs). Under the SDoC process, the responsible manufacturer or importer only needs to make a self-determination that the equipment complies with the FCC's technical standards and must make testing information available to the FCC upon request. Some devices are exempt from the certification and SDoC processes because their potential for causing harmful interference is so low, such as devices with very low power consumption or that generate very low frequencies.

New Equipment Authorization Rules

On November 25, 2022, the FCC released a Report and Order (R&O) in which it adopted new equipment authorization rules (EA Rules) prohibiting authorizations for equipment on the Covered List (Covered Equipment). While these rules are the culmination of a rulemaking proceeding begun in June 2021, they also implement the Secure Equipment Act of 2021. The Secure Equipment Act took effect in November 2022 and directs the FCC to adopt rules that "clarify" that the Commission will "no longer review or approve" authorizations for equipment on the Covered List.

The EA Rules require all applicants using the certification process to attest that the application is not for Covered Equipment. They also prohibit companies named on the Covered List from using the SDoC process or from relying on an exemption for their equipment, even if that equipment is not Covered Equipment. The FCC explained that this requirement will secure its oversight over these companies and prevent evasion of the prohibition on Covered Equipment. While the FCC did not revoke *prior* authorizations for Covered Equipment, it did assert its authority to do so and asked for comments on whether and how it should do so. It also asked for comments on whether and how it should withhold authorization for component parts (i.e., pieces of equipment that are used within a finished product) manufactured by entities named on the Covered List.

As the R&O explains, Covered Equipment currently includes "telecommunications equipment" and "video surveillance equipment" produced by Huawei, ZTE, Hytera, Hikvision, and Dahua. According to the R&O, "telecommunications equipment" broadly encompasses any equipment that can be used in a broadband network, including consumer electronic devices that exchange data over the internet. "Video surveillance equipment" encompasses any device that enables users to originate and receive high-quality video service over broadband internet, such as surveillance cameras, body cameras, and data storage devices for video surveillance. Any telecommunications or video surveillance equipment produced by Huawei or ZTE is Covered Equipment; by contrast, equipment produced by Hytera, Hikvision, and Dahua is only considered Covered Equipment if it is used for a prohibited purpose (such as security of government facilities, surveillance of critical infrastructure, and other national security purposes). Still, the FCC announced that it would not approve any telecommunications or video surveillance equipment made by these three companies unless they first submit a plan for the FCC's approval outlining how they will ensure the equipment is not marketed or sold for a prohibited purpose.

Potential Legal Challenges

Interested parties impacted by the EA Rules will have 30 days from the R&O's publication in the Federal Register (FR) to file a legal challenge in a federal appellate court. As the R&O has not yet been published in the FR (publication is delayed due to the need for Office of Management and Budget review under the Paperwork Reduction Act), it remains to be seen whether it will be litigated.

Should the EA Rules be challenged in court, the litigation might focus on arguments that the rules exceed the FCC's statutory authority. For instance, during the rulemaking, Hikvision maintained that the FCC did not have statutory authority to ban video surveillance equipment because it is "peripheral" customer premises equipment rather than essential to communications networks. Hikvision argued that banning this

type of equipment would be "so unprecedented" that, under the major questions doctrine, the FCC needs explicit authorization from Congress to do so.

Litigants might also challenge the rules on constitutional grounds. Commenters proffered various constitutional arguments during the rulemaking, including that the rules violate the Equal Protection Clause, are an unconstitutional taking of property, and violate separation of powers. The argument most commonly made, however, is that the restrictions are an unconstitutional "bill of attainder" (i.e., legislative punishment). Under U.S. Supreme Court precedent, a law is an unconstitutional bill of attainder if it (1) specifically targets individuals or groups and (2) inflicts punishment without a trial. Objecting companies may have particular difficulty establishing that the restrictions inflict punishment. In Huawei's challenge to the 2019 NDAA, a federal district court held that the statute's restriction did not amount to punishment because the law reasonably furthered non-punitive goals, such as protecting national security and informational security. The D.C. Circuit reached a similar conclusion in its 2018 decision in *Kaspersky Lab, Inc. v. DHS*, which dealt with the 2017 NDAA's prohibition on government agencies using "hardware, software, or services" developed by the Russian cybersecurity company Kaspersky Lab. For more discussion of these cases, see CRS Legal Sidebar LSB10274, *Huawei v. United States: The Bill of Attainder Clause and Huawei's Lawsuit Against the United States*, coordinated by Joanna R. Lampe.

Considerations for Congress

Over the past several years, Congress has played an active role overseeing the FCC's approach to securing the nation's communications networks, in particular by passing the Secure Networks Act and the Secure Equipment Act. Congress could continue to shape the FCC's efforts in this space and might address some of the outstanding issues around equipment authorizations.

For instance, the FCC is considering whether to revoke prior authorizations for Covered Equipment, but has not yet done so. If Congress believes that revoking prior authorizations is undesirable because, for instance, it might limit consumer options for affordable electronic equipment or impact the supply chain, it could prohibit the FCC from taking this step. Alternatively, Congress could require the FCC to revoke prior authorizations for Covered Equipment if it believes doing so is necessary for network or national security.

Should Congress require revocation, one consideration is that revoking prior authorizations might implicate the U.S. Constitution's Due Process Clause. Under the Due Process Clause, the government may not deprive any person of their property without notice of the government action and a meaningful opportunity to contest it. Government benefits or licenses may be considered property interests under the Due Process Clause if they give the recipient a "legitimate claim of entitlement" to the uninterrupted enjoyment of the benefit. While courts have not said whether companies have a constitutionally protected property interest in FCC equipment authorizations, legislation that empowers the FCC to revoke authorizations without notice and an opportunity to respond could raise due process challenges. Affected companies might also argue that revoking prior authorizations without compensation violates the Constitution's Takings Clause. The Takings Clause prohibits the government from "tak[ing] property for public use, without just compensation." It is unlikely that the equipment authorizations themselves would be property under the Takings Clause, as courts have generally been skeptical of arguments that government licenses are property for Takings Clause purposes. Affected companies may argue, however, that a revocation is a "regulatory taking" if it results in serious financial loss in a way that frustrates their reasonable investment-backed expectations. Congress may seek to shift the burden for future authorizations by establishing a timeframe in which an authorization or transfer sunsets, similar to the way broadcast licenses are granted for a defined duration, rather than allowing a grant of the authorization in perpetuity, thereby potentially limiting future revocation actions.

Congress might also address whether the FCC should deny authorizations for equipment with component parts produced by entities on the Covered List. The FCC said that component parts produced by these entities could pose an unacceptable national security risk, and the agency is exploring how to address this issue. Some commentators, such as the Internet & Television Association (NCTA), have argued that the FCC's equipment authorization authority is limited to finished products and that extending the prohibition to component parts would burden small companies with limited ability to identify the manufacturer of every component in a given piece of equipment. Congress might weigh in, for instance, by passing legislation clarifying whether and how the FCC should approach component parts in the authorization process.

Author Information

Chris D. Linebaugh
Legislative Attorney

Disclaimer