Cooley

Court Instructs FCC to Amend Definition of 'Critical Infrastructure' in Equipment Authorization Order

April 9, 2024

The US government has made efforts to combat national security threats found in technology. Notably, the Federal Communications Commission (FCC) and Congress worked in tandem to create a **Covered List of communications equipment and services** that pose a threat to US national security. Companies on the Covered List cannot obtain new equipment authorizations required to sell new or updated products in the US. Two companies – Hikvision USA and Dahua Technology USA – recently challenged the FCC's order that implemented a ban on their video surveillance equipment in the use of security critical infrastructure.

In a **recent decision**, the US Court of Appeals for the District of Columbia Circuit upheld the FCC order prohibiting authorization of Covered List equipment from being used for "physical security surveillance of critical infrastructure." However, the court instructed the FCC to change its definition of "critical infrastructure" in the order, because as currently written the definition is overbroad.

The following summary describes a history of the Covered List and a summary of the petitioners' challenge to their equipment being placed on the Covered List.

History of the Covered List

The Covered List is a list of communications equipment and services that are "deemed to pose an unacceptable risk to the national security of the United States." In 2020, Congress passed the Secured and Trusted Communications Networks Act (SNA), instructing the FCC to create the Covered List and publish the list on its website. To adhere to the requirements of the SNA, the FCC issued the Supply Chain Second Order, which "established procedures and criteria for compiling the Covered List." The following year, the FCC published the Covered List and issued a notice of proposed rulemaking (NPRM) proposing to ban the authorization of equipment on the Covered List. Congress subsequently passed the Secure Equipment Act (SEA) requiring the FCC to adopt the **equipment authorization rules proposed in the NPRM** and enact an equipment authorization ban for items on the Covered List. The FCC issued the order banning equipment authorizations for "covered equipment," which meant that companies on the Covered List no longer could put new products on the market in the US. The FCC determined that Hikvision's and Dahua's video surveillance technologies would be included on the Covered List to the extent that they were "used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."

The appeal

In their appeal, Hikvision and Dahua challenged the order, arguing that the FCC exceeded the scope of its statutory authority when it placed their equipment on the Covered List, and that the FCC's definition of "critical infrastructure" was overbroad and inconsistent with the law.

Statutory authority

Hikvision and Dahua argued that the FCC misconstrued the SNA when placing their products on the Covered List, and that even though the Supply Chain Second Order no longer could be challenged, they could challenge the definition in this case because the FCC reopened the definition of covered equipment in the 2022 order. However, the court noted that Congress was aware that the petitioners' products were on the Covered List and set to be banned under limited purposes. The court found that Congress intended for the FCC to prohibit the marketing and sale of Hikvision's and Dahua's products, holding that the SEA "ratified the composition of the Covered List" and did not permit Hikvision or Dahua to challenge the placement of its products on the list.

Definition of 'critical infrastructure'

The FCC's order banned the use of Hikvision's and Dahua's equipment when used for "the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." The FCC's order concluded that any systems or assets that are physically or virtually "connected to" various government systems could reasonably be considered "critical infrastructure." The FCC relied on the Patriot Act's definition of critical infrastructure and incorporated 16 sectors in Presidential Policy Directive 21 and 55 National Critical Functions from the Cybersecurity and Infrastructure Security Agency National Risk Management Center's risk management guide that could be considered "critical infrastructure."

Hikvision and Dahua challenged the FCC's interpretation, arguing that it contravened congressional intent "by treating nearly all aspects of the economy as 'critical infrastructure.'" The court agreed. It held that the FCC's reliance on prior government sources to define critical infrastructure was reasonable, but that the FCC did not "explain or justify its use of the expansive words 'connected to,'" which made the definition "arbitrarily broad." The court vacated the portions of the FCC's order defining "critical infrastructure" and instructed the FCC to "comport its definition and justification for it with the statutory text of the NDAA [National Defense Authorization Act]."

Implications of the decision

The court decision makes clear that the petitioners' video surveillance equipment will remain on the Covered List; however, the extent to which it will be prohibited may narrow when the FCC reconsiders its definition of "critical infrastructure." Moreover, Hikvision and Dahua will still require FCC approval of individual marketing plans mentioned in the decision, which is unlikely to occur until the FCC revises its definition of critical infrastructure. Until then, the companies cannot obtain authorization for the types of equipment covered by the FCC's 2022 order.

This case adds to the FCC's numerous proceedings to develop new rules and programs to enhance the cybersecurity of consumer equipment in the US. For more information on this case or the FCC's work in this area, please contact one of the attorneys listed below.

Key Contacts

Henry Wendel Washington, DC	hwendel@cooley.com +1 202 776 2943
J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818
Belen Crisp Washington, DC	bcrisp@cooley.com +1 202 776 2289