

Commerce Department Further Clamps Down on Huawei

By [John B. Reynolds](#), [Will Schisa](#), [Joseph Kniaz](#) & [Genevieve A. Lewis](#) on August 19, 2020

POSTED IN [ADMINISTRATIVE LAW](#), [CFIUS](#), [ECONOMIC SANCTIONS](#), [GUIDANCE & FAQs](#)

On August 17, 2020, the Bureau of Industry and Security (BIS) at the Department of Commerce **announced** it was tightening restrictions on Huawei's access to American technology through a new **rule** that: (1) further amends BIS' foreign direct product (FDP) rule to restrict Huawei's access to items produced using U.S.-origin technology, software, or equipment; (2) adds a number of additional Huawei affiliates to BIS' Entity List; and (3) removes a temporary general license (TGL) that had authorized certain limited transactions involving Huawei and its affiliates, while making permanent a very narrow general license relating to cybersecurity and vulnerability research. According to the Commerce Department, the new rule aims to prevent Huawei from evading the Export Administration Regulations (EAR) by using third party affiliates and convoluted transactions. These restrictions are part of an increased anti-China regulatory posture by the United States, particularly in the telecommunications space, on the basis of national security. The rule is scheduled to be published in the *Federal Register* on August 20, 2020, and became effective upon being made available for public inspection on August 17, 2020.

FDP Rule Changes

These restrictions expand upon BIS' May 2020 amendment to the FDP Rule, which we described in a prior **[blog post](#)**. The May amendment was written to target Huawei's acquisition of semiconductors that are the direct product of U.S. technology and software by imposing licensing requirements on the export, reexport, or transfer to Huawei affiliates named on the Entity List of: (1) foreign manufactured items produced or developed by Huawei that are the direct product of software or technology subject to the EAR and classified under specific Export Control Classification Numbers (e.g., 3E001, 5D001); or (2) foreign manufactured items that are the direct product of software or technology produced or developed by Huawei and produced by any plant or major component of a plant that is located outside the United States, where that plant or its component is a direct product of U.S.-origin

software or technology subject to the EAR and classified under the same export classification numbers.

Due to U.S. government concerns about Huawei attempting to get around the May restrictions, and in response to public comments, BIS is broadening this restriction in two key ways. First, it is removing the requirement that the specified items described above be “produced or designed” by Huawei in order to be subject to a licensing requirement. Second, it is expanding the licensing requirement to all transactions in which the item will be incorporated into, or will be used in the production or development of any part, component, or equipment produced, purchased, or ordered by a listed Huawei entity, or where a listed Huawei entity is a party to the transaction, whether as purchaser, end-user, or intermediate or ultimate consignee. In a concurrently published [rule](#), BIS is amending the Entity List to clarify that this latter point – that the restrictions applicable to parties on the Entity List apply regardless of their role in a transaction – applies generally and is not specific to Huawei.

Listing of Additional Huawei Affiliates

The rule will also add an additional 38 Huawei affiliates in 21 countries to the Entity List, in addition to the 69 entities [originally listed](#) in May 2019 and 46 affiliates [added](#) in August 2019. The newly added affiliates are principally entities in Huawei’s cloud and Open Lab business lines. The Commerce Department found that there was reasonable cause to believe that Huawei otherwise would seek to use these affiliates to evade the restrictions imposed by the Entity List.

Removal of TGL

Shortly after the initial inclusion of Huawei on the Entity List, BIS issued a TGL authorizing certain limited classes of transactions involving Huawei and its affiliates, as described in our May 2019 blog post. The TGL has been consistently extended, with some modifications. At the time of the most [recent extension](#), in May 2020, BIS signaled that it expected to remove or modify the TGL after August 13, 2020. BIS has now followed through on this, removing the TGL and replacing it with a narrow, permanent authorization covering only one of the categories of activities previously covered by the TGL, specifically exports, reexports, or transfers of technology subject to the EAR for cybersecurity research and vulnerability disclosure, when the disclosure to Huawei and/or to its listed non-U.S. affiliates is

limited to information regarding security vulnerabilities in items owned, possessed, or controlled by Huawei or any of its non-U.S. affiliates when related to the process of providing ongoing security research critical to maintaining the integrity and reliability of an existing and currently fully operational third-party network and equipment.

These actions are part of a larger regulatory push to control access to American technology in foreign supply chains and in particular scrutinize Chinese telecommunications companies. For instance, last year the Federal Communications Commission **barred** state-owned China Mobile from operating domestically. In April of this year, the Trump administration recommended both that the U.S. **revoke** a license for a subsidiary of China's largest landline company and **deny** Google permission to run high-speed Internet cable to Hong Kong. In July, the Department of Defense, the General Services Administration, and the National Aeronautics and Space Administration issued **interim regulations** that effectively prohibit these agencies from contracting with companies that use Huawei and other Chinese company technologies. And the U.S. State Department continues to promote its "**Clean Network Initiative**" aimed at encouraging foreign partners and private companies to take steps to exclude Huawei and other Chinese actors the U.S. government believes to pose security or privacy concerns.

Proprietary technology and telecommunications power have become a key national security battleground. This month's restrictions on Huawei are a clear bellwether of escalating U.S.-China regulatory distrust.