wiley

NEWSLETTER

Foreign Telecom Deals to Be Restricted Under Sweeping New Order Targeting U.S. Network Supply Chain Security

June 2019

Privacy in Focus®

The technology and communications sectors are facing increasing scrutiny and regulation focused on U.S. network supply chain security in order to address what a recent Executive Order calls "malicious cyber-enabled actions" and "economic and industrial espionage." President Trump last month signed a long-anticipated Executive Order authorizing the Secretary of Commerce to regulate and prohibit transactions involving information and communications technology and services that are produced or supplied by "foreign adversaries." While the Order does not explicitly single out any particular country or company, it is widely believed to be aimed at Huawei and other Chinese telecommunications companies. The U.S. Department of Commerce's (Commerce) Bureau of Industry and Security (BIS) simultaneously placed Huawei and 68 of its affiliates on BIS's Entity List, prohibiting nearly all U.S. exports to them.

Long-Anticipated Executive Order Will Prohibit U.S. Companies from Buying Foreign Telecom Equipment and Services Deemed to Pose a National Security Threat

The Executive Order declares a national emergency to combat U.S. national security threats such as "malicious cyber-enabled actions" and "economic and industrial espionage." The Order, which is potentially sweeping in scope, broadly prohibits any acquisition, importation, transfer, installation, dealing in, or use of any "information and communications technology or service" where Commerce finds that "the transaction involves information and

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Daniel P. Brooks
Partner
202.719.4183
dbrooks@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary," and the transaction:

1. poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;
2. poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
3. otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

The term "information and communications technology or services" is not limited to 5G technology and services and is defined broadly to include "any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display." The Order authorizes Commerce to issue licenses to authorize specific transactions and provides Commerce with discretion to design or negotiate mitigation measures to address any concerns "as a precondition to the approval of a transaction or of a class of transactions" that would otherwise be prohibited.

The Order directs Commerce to publish implementing regulations within 150 days of the date of the Order – i. e., by October 12, 2019 – and the National Telecommunications and Information Administration (NTIA) is expected to take a lead role. Such regulations may:

- Determine that particular countries or persons are foreign adversaries;
- Identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries;
- Identify particular technologies or countries with respect to which transactions involving information and communications technology or services warrant particular scrutiny;
- Establish procedures to license transactions otherwise prohibited pursuant to the Order;
- Establish criteria by which particular technologies or particular participants in the market for information and communications technology or services may be recognized as categorically included in or as categorically excluded from the prohibitions of the Order; and
- Identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with a particular transaction.

The Executive Order also directs agencies to produce periodic assessments and reports about threats to the information and communications technology sector, and hardware, software, and services used by critical infrastructure. Federal agencies may need and seek assistance from the private sector with these assessments.

The Order is expected to particularly affect rural telecommunications operators, which tend to use Huawei network equipment due to its comparatively low cost. Recognizing that replacing Huawei equipment would be potentially cost-prohibitive for most rural carriers, a bipartisan group of Senators recently introduced the 5G Leadership Act, which would set aside up to $700 million from future spectrum auctions to help U.S. communications providers remove Huawei equipment from their networks.

Commerce Bans U.S. Exports to Huawei

In another major blow to Huawei, BIS added Huawei and 68 of its affiliates to its Entity List, which will have considerable ramifications on the Chinese company as well as the global telecommunications industry and consumers. BIS's ban prohibits nearly all U.S.-origin exports of hardware, software, and technology to Huawei, including software and software updates/patches (unless such software is publicly available), electronic parts and components such as chips and routers, and related technology (again, unless that technology is publicly available). From a practical standpoint, users and operators may not be able to receive updates and patches for Huawei network equipment and handsets to the extent such updates or patches are provided from U.S. entities and routed through or customized by Huawei. The sweeping prohibitions also extend to the provision of parts, components, software, or other items that would be used to service or repair equipment already owned by Huawei. Additionally, foreign companies that incorporate U.S. parts and components into their products must carefully assess whether those products are subject to U.S. controls based on their U.S. content, as such products also could fall under the restrictions on Huawei.

BIS has issued a temporary general license effective through August 19, 2019, permitting the following transactions that otherwise would be prohibited:

1. *Continued operation of existing networks and equipment* – Companies are permitted to engage in any transactions necessary to maintain and support existing and currently fully operational networks or equipment (e.g., software updates and patches) that were subject to legally binding contracts/agreements executed between a listed Huawei entity and third parties on or before May 16, 2019.
2. *Support* to existing handsets – Companies also can engage in transactions necessary to provide service and support (e.g., software updates or patches) to existing Huawei phones; this provision covers models of Huawei phones that were available to the public on or before May 16, 2019.
3. *Cybersecurity research* and vulnerability disclosure – Companies can disclose to the listed Huawei entities information regarding security vulnerabilities in items owned, possessed, or controlled by a listed entity as part of an effort to provide ongoing security research that is critical to maintain the integrity and reliability of existing and currently fully operational networks and equipment.
4. *Engagement as necessary* for 5G standards by a duly recognized standards body – The temporary general license also permits engagement with the listed Huawei entities as necessary for the development of 5G standards as part of a duly recognized international standards body.

As national security concerns increasingly push the federal government to disrupt settled business relationships, companies must grapple with greater uncertainty in long-term planning. The challenge will be not just to understand and manage the current restrictions on Huawei, but also to be prepared for the possibility that the federal government will take actions that may fundamentally alter other aspects of the global supply chain.