

CLIENT ALERTS

What U.S. Sanctions against Huawei Mean for the Future

5.21.2019

On May 15, 2019, President Trump issued a new Executive Order widely reported as being targeted against Huawei to keep it from doing business in the United States. That same night, the Department of Commerce put Huawei on the "Entity List," which makes it more difficult for United States companies to sell or export goods or services for Huawei's use. These two measures have drawn extensive coverage, but not as much has been written about how they might affect international transactions more generally. They were triggered by deep concerns in the U.S. intelligence community and among U.S. policy makers that Huawei is beholden to the Chinese government. Policy makers fear that using Huawei products to construct a 5G cellular telecommunications network would leave the host country vulnerable to spying by the Chinese government.

But these moves are not limited to Huawei alone, nor are they confined to actions taken by the Chinese government. Instead, they portend a broader approach that could affect your company even if you have no dealings with Huawei or with China. Here are a few things every company doing business internationally needs to know.

First, the President's Executive Order affects only *imports* and transactions within the United States. It concentrates primarily on transactions in which Huawei is the supplier. The Commerce Department addition of Huawei to its "Entity List," on the other hand, affects only *exports* and associated transactions. It concentrates primarily on deals in which Huawei is a customer or recipient of information and communications technology. Because these two actions aim at different segments of the economy, they are worth analyzing separately.

New Executive Order

Related People

Joseph G. Cosby
Of Counsel

Related Services

International Business

International Trade and
Customs Specialty Team

CLIENT ALERTS

The new executive order issued by President Trump creates a whole new administrative enforcement mechanism for dealing with national security threats that emanate from a particular sector of the economy. To begin with, the agency charged with drafting the new regulations and enforcing the new sanctions is not the Department of Treasury Office of Foreign Assets Control (“OFAC”), as is most common, but the Department of Commerce. Although the executive order does not specify which subdivision of the Department of Commerce will be responsible, it will most likely be the Bureau of Industry and Security (“BIS”), the agency responsible for the Entity List. This is noteworthy because OFAC has typically been the office charged with responsibility for U.S. sanctions programs aimed against countries, companies, and individuals that the president concludes are a threat to United States national securities interests. BIS is typically tasked with enforcing regulations to ensure that U.S. technology that has both commercial and military applications does not fall into the wrong hands. At the same time, BIS does have some involvement in administering sanctions programs aimed at specific individuals, companies, and other entities, so this choice is not too surprising.

In addition, the new executive order structures the new sanctions much differently than the sanctions OFAC most commonly enforces. The new sanctions regime announced by the executive order focuses on “foreign adversaries” rather than clearly identified countries or groups that post a threat; on individuals and companies that are controlled or directed by these unnamed foreign adversaries, rather than individuals and companies that engage in specified prohibited transactions or activities; and on “transactions” in a specified economic sector (“information and communications technology”), rather than on broad-based property interests either present in the United States or connected to an individual or entity governed by U.S. law. To be more specific, the executive order requires U.S. persons to obtain a license from the Department of Commerce in order to engage in “transactions” involving “information and communications technology” with persons or companies “owned by, controlled by, or subject to the direction or jurisdiction” of “foreign adversaries.”

First, the executive order does not specify who the “foreign adversaries” are and leaves that task to the Department of Commerce, acting in consultation with the Department of State, the Department of the Treasury (which houses OFAC and the Financial Crimes Enforcement Network, also a part of the U.S. foreign intelligence community), and other agencies. Although the executive order does not name Huawei, it is generally understood that the order was issued in part to address the national security threat that intelligence agencies perceive from Huawei and China. So we can assume that when the final regulations are issued, the Department of Commerce will designate China as a foreign adversary. But the executive order is broad in this respect, and nothing stops the Department of Commerce from ultimately designating other countries or even other entities (such as ISIS) as “foreign adversaries.”

Second, the executive order is not limited to Huawei alone. Once again, the executive order grants the Department of Commerce the authority to designate individuals or companies considered to be “owned by, controlled by, or subject to the jurisdiction or direction” of a foreign adversary. There has already been speculation that the Department of Commerce could designate ZTE in addition to Huawei, although for now it is only speculation. But the broad authority that the executive order grants to the Department of Commerce should not be ignored, and the designations that the Department

CLIENT ALERTS

makes will be watched with interest.

Third, the executive order applies to “transactions,” which it defines as “any acquisition, importation, transfer, installation, dealing in, or use” of information and communications technology or services. Under the executive order, anyone who acquires, imports, installs, or uses the relevant goods or services after May 15, 2019, must first obtain a license from the Department of Commerce. The executive order sweeps broadly to include quite a few activities companies engage in after they have purchased goods and services. On May 20, 2019, BIS issued a temporary, 90-day license allowing companies affected by the addition of Huawei and its affiliates to the Entity List to continue to maintain and support existing and fully operational networks and equipment and to take other actions.

But the license applies only to those affected by Huawei’s addition to the Entity List, which affects only those companies that sell or supply goods, services, and information to Huawei. This license does not affect organizations that may have purchased, installed, or used Huawei goods or services. Huawei’s customers do not yet need to cut ties with Huawei because the Department of Commerce has not yet designated Huawei as a person subject to the control or direction of a foreign adversary. But when that time comes, the Department of Commerce is unlikely to grant anything longer than a short temporary license to give companies a little breathing room to unwind their relationship with Huawei. For many of those companies, it may make sense to start that process now.

Fourth, the sanctions on Huawei and others could well expand beyond the borders of the United States. U.S. companies could, for instance, be prohibited from participating in efforts to build a 5G network in Great Britain, which has already signaled its willingness to use Huawei products and assistance to build that network. We will not know how far the sanctions will reach until we see the proposed regulations and enforcement policies.

One factor potentially limiting the scope of the sanctions against Huawei is the licensing feature in the new executive order. As noted above, the executive order does not flatly ban U.S. companies from engaging in any transactions subject to the executive order sanctions, but only those transactions for which the U.S. companies do not have a license from the Department of Commerce. The executive order leaves it up to the Department of Commerce to determine the general tenure of its licensing policy and to make exceptions, where appropriate, to the prohibitions articulated in the executive order. The general license that BIS issued on May 20 suggests that the Department of Commerce will enforce the executive order aggressively, but with some breathing room to accommodate certain interests necessary to maintain existing networks and keep them secure. However, we won’t know until Commerce designs and begins to implement its licensing policy.

Adding Huawei to the Entity List

If your company supplies any goods, services or technical information to Huawei, or exports goods or services that you know ultimately reach Huawei, you would be well-advised to seek legal counsel to determine whether you need a license from BIS to continue. The Entity List covers primarily transactions in items that are covered by the Export Administration Regulations (“EAR”), which applies

CLIENT ALERTS

primarily to "dual-use" items that have both civilian and military uses. But even some items that don't qualify as a "dual-use" are still be covered by the EAR under certain circumstances. And even the products your company supplies to Huawei (directly or indirectly) are not covered by the EAR, the Commerce Department still treats any business transactions with Huawei as a "red flag." That "red flag" requires companies to use special caution before entering or completing a transaction with Huawei, and it significantly increases the risk that the company will be subject to a government investigation or enforcement action.

The general license that BIS issued on May 20, 2019, reinforces the need for caution. While the license permits many useful activities – such as allowing companies to continue to operate and support existing, fully operational networks and equipment; to provide support, including software updates or patches, to existing handsets that were available to the public on or before May 16, 2019; to disclose security vulnerabilities to Huawei as part of an effort to maintain the integrity and reliability of fully operational networks and equipment; and to engage in international standards bodies (e.g., IEEE and ISO) to develop 5G standards – it is still only a temporary license that expires in 90 days (on August 19, 2019).

While the Department of Commerce is likely to replace the temporary license with a more permanent framework for addressing some issues, such as the structures necessary to keep existing networks and equipment secure and functioning, the license for other activities might not be extended. Companies engaging in activities that are not granted an extension when the current 90-day license expires will either need individual licenses or will need to have terminated their relationship with Huawei. The bottom line is that if you have an existing supply arrangement with Huawei or a company that you know (or have reason to know) supplies Huawei, you should check with a lawyer.

Conclusion

The dual announcements on May 15, 2019, open a new chapter in U.S. sanctions policy and relationships with China and, more particularly, Huawei. Butzel Long will continue to monitor future developments closely and to bring you up-to-date as warranted. If you have any questions concerning how these or other developments affect you or your company, please do not hesitate to contact your regular Butzel Long attorney or the author of this alert.

Joseph G. Cosby

202.454.2880

cosby@butzel.com