COVINGTON

# National Security Update: President Trump Signs Executive Order on Information and Communications Technology Supply Chain; Commerce Department Adds Huawei to Entity List

May 16, 2019

---

## SUMMARY

We are writing to provide an update on two important developments in U.S. national security-based regulation of trade: (1) a new, potentially expansive Executive Order on information and communications technology supply into the U.S. market, and (2) the Department of Commerce's action to add Huawei to the Entity List.

President Donald Trump yesterday signed an executive order (the "Order") entitled "Securing the Information and Communications Technology and Services Supply Chain." The Order declares a national emergency with respect to threats against information and communications technology ("ICT") and services in the United States, and delegates authority to the Secretary of Commerce to prohibit transactions posing a risk to U.S. national security. The President declared this national emergency under the authorities granted in the International Emergency Economic Powers Act ("IEEPA"), the National Emergencies Act (50 U.S.C. § 1601 et seq.), and section 301 of title 3, United States Code (relating to delegation of powers).

There are four key points to understand regarding the Order. First, although the Order may be framed publicly as an escalation in the Trump Administration's trade war with China, the reality is that the Order has been in the works for several years. It had its origins in the Obama Administration, and emanates out of U.S. national security concerns about the ability of foreign adversaries to exploit the supply chain to critical infrastructure, which is under the ownership and control of the private sector—not the government—in the United States.

Second, notwithstanding that the concept of the Order has in fact been circulating for years, the Order as ultimately issued by President Trump is much broader than original conceptions and is sweeping in its potential scope. It theoretically authorizes the U.S. government to prohibit or condition nearly any transaction, by any person or with respect to property subject to U.S. jurisdiction, involving information and communications technology or services by persons owned, controlled, or subject to the jurisdiction or direction of a "foreign adversary," and that pose a national security threat.

Third, although publicly discussed as targeting the security risks posed by supply from Chinese telecommunications equipment firms—which was the original motivation for the Order—the Order in fact does not specify any country or any company, and could be applied more widely.

Fourth, given the breadth of the Order, there is significant ambiguity and uncertainty regarding how it will actually be applied. Thus, the rulemaking authorized under the Order—with the Secretary of Commerce directed to adopt rules within 150 days—will be crucial. In the narrowest sense, the Order simply could enable the U.S. government to have a veto over private sector procurement of technology or services from a select group of vendors. However, if the full potential of the Order is implemented, it could establish an entirely new regulatory regime for private sector procurement of information and communications technology and services in critical infrastructure—essentially, a supply chain procurement version of the CFIUS process for foreign investment.

The Order is the latest in a series of actions taken by the U.S. government to address concerns about national security risks arising from commercial transactions. These actions include the enactment of the Foreign Investment Review Modernization Act (FIRRMA), which transformed the authorities of the Committee on Foreign Investment in the United States (CFIUS); the Export Control Reform Act (ECRA), which created a formal interagency process to identify emerging and foundational technologies "essential to the U.S. national security" warranting export control; and Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY19 NDAA) prohibiting the use by the U.S. government of certain telecommunications and video surveillance services or equipment. (The Department of Defense has yet to issue an interim or final rule for this section.)

Separately, the Department of Commerce, Bureau of Industry and Security ("BIS") has amended the Entity List of restricted persons to include Huawei Technologies Co. Ltd. ("Huawei") and Huawei affiliates. The formal BIS rule, released today, adds to the Entity List Huawei and 68 non-U.S. Huawei affiliates spread across 26 countries worldwide. While the rule will not be published until May 21, it is immediately effective upon release. All exports, re-exports, and transfers (in-country) to the listed Huawei entities of any item subject to the Export Administration Regulations ("EAR") now require prior BIS licensing. License exceptions under the EAR are now suspended with regard to exports to Huawei and BIS has instituted a license review policy of a presumption of denial of export license requests. We will issue a further alert on this topic shortly.

With that as background, we turn to a fuller discussion of the Executive Order.

## Principal Elements of the Executive Order

Broadly speaking, the Order prohibits U.S. entities from purchasing, using, or dealing in any ICT product or services from a "foreign adversary" if there is a risk to U.S. national security. Specifically, it applies to ICT, including ICT services, "designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." ICT is defined as "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 also defines "foreign adversaries" broadly as entities "engaged in a long-term pattern or serious instances of conduct significantly adverse" to U.S. national security. The Order

prohibits U.S. entities from acquiring, importing, transferring, installing, dealing in, or using such technology or services if the transaction poses an "undue risk" of sabotage to U.S. information and communications technology or of "catastrophic effects" to critical infrastructure, or if it "otherwise poses an unacceptable risk" to U.S. national security.

The Order, however, does not indicate precisely what technology or services will be subject to this restriction. Nor does it indicate which products or companies will be deemed to be controlled by adversaries and "warrant particular scrutiny"; how such technology or services will be identified; whether and how the Order will be enforced; and exactly which entity within the Department of Commerce ("Commerce") will be responsible for this regime. Rather, the Order authorizes the Secretary of Commerce—informed by an inter-agency consultation process to include the Secretary of the Treasury, Secretary of State, Secretary of Defense, Attorney General, Secretary of Homeland Security, U.S. Trade Representative, Director of National Intelligence, Administrator of General Services, Chairman of the Federal Communications Commission, and heads of other agencies, as appropriate—to direct the "timing and manner" of the cessation of transactions that it prohibits. It also mandates that Commerce, again in consultation with the other agencies, adopt "appropriate rules and regulations," such as identifying "particular countries or persons" as foreign adversaries and identifying persons "owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries" under the Order. It may also establish procedures to license transactions otherwise prohibited pursuant to the Order; set out criteria by which particular technologies or participants in the market for ICT may be recognized as categorically included or excluded from the Order's prohibitions; and identify a mechanism and relevant factors for negotiating agreements to mitigate concerns that the Order identifies.

Notably, the Order is not limited to products, but also extends to services. It would thus potentially allow the U.S. government to prohibit U.S. companies from using certain service providers. The inclusion of service providers in the scope of the Order likely reflects concerns that have developed in recent years within U.S. national security agencies about risks that may be introduced through service providers, and especially managed network service providers in the telecommunications industry. Whether or not the authority of the Order will be used in that fashion is yet to be seen.

The Order contemplates that the U.S. government also will provide paths for procurement of technology and services that otherwise would be restricted. In doing to so, it seemingly borrows concepts both from the U.S. export control regime and from the CFIUS and "Team Telecom" process for addressing national security risks arising from foreign investment.

To accomplish this, the Order delegates authority to the Secretary of Commerce to license transactions otherwise proscribed by the Order. The Secretary is further authorized under the Order to establish criteria by which to identify particular information and communications technologies and persons subject to or exempt from the Order's prohibitions.

The Order also expressly permits the Secretary of Commerce to "design or negotiate measures to mitigate" any identified concerns. This provision effectively permits the government to regulate the use of foreign service and technology providers by U.S. companies by requiring mitigation measures as a condition of use. U.S. national security agencies have already been leveraging other authorities, including CFIUS and "Team Telecom" reviews, to extract commitments from U.S. parties on the use of foreign technology and service providers. The Order potentially allows the U.S. government to expand those requirements more broadly.

Commerce must publish the rules setting forth the regime required under the Order within 150 days of the Order—no later than October 12, 2019. However, it is uncertain that the agencies in fact will have the resources and ability to meet this deadline. Much of the expertise in the agencies on these issues also resides with the components who are responsible for Team Telecom and CFIUS, and they already are stretched thin by their caseload and the rulemaking required under FIRRMA. Moreover, the government is still in the process of implementing related supply chain security provisions from the FY19 NDAA, which became law on August 13, 2018. The interagency coordination process will also add an element of complexity.

Finally, the Order directs several reports to Congress. Within a year of the Order, and annually thereafter, Commerce must submit a report to the President assessing whether the actions taken under the Order sufficiently address the risks that it identifies. The Order also requires the Office of the Director of National Intelligence to produce a report within 40 days assessing threats from technology produced or controlled by foreign adversaries, and annually thereafter. Further, the Department of Homeland Security must produce a report within 80 days (and also annually thereafter) on the vulnerabilities present in hardware, software, and services that "pose the greatest potential consequences" to U.S. national security.

## Implications and Next Steps

Given its breadth, the full implications of the Order will not be known until Commerce publishes its rules. Although public discussion of a potential "supply chain" executive order has emphasized U.S. government concerns with China, under the Order, Commerce is authorized to name a much larger list of countries as adversaries and to establish rules and regulations that would go well beyond simply regulating procurement of ICT products and services from Chinese firms.

Regardless of how the U.S. government implements the Order, it is significant in that the Order represents the first broad attempt by the U.S. government to regulate the entire U.S. supply chain for information and communication technologies and services. Even as Commerce adopts and applies regulations, it will take time for the U.S. government to determine how to conduct effective oversight and balance security concerns against the potential economic and trade-related effects of the Order.

We will be closely following the regulations development process, and will keep our clients updated.

* * *

We hope that you find this report useful. Please do not hesitate to contact the following Covington attorneys and advisors if you would like to discuss any aspect of the foregoing in further detail:


| | | |
|---|---|---|
| **Mark Plotkin** | +1 202 662 5656 | mplotkin@cov.com |
| **David Fagan** | +1 202 662 5291 | dfagan@cov.com |
| **Peter Lichtenbaum** | +1 202 662 5557 | plichtenbaum@cov.com |
| **Trisha Anderson** | +1 202 662 5048 | tanderson@cov.com |
| **Yaron Dori** | +1 202 662 5444 | ydori@cov.com |
| **Matthew DelNero** | +1 202 662 5543 | mdelnero@cov.com |
| **Gerard Waldron** | +1 202 662 5360 | gwaldron@cov.com |

| | | |
|---|---|---|
| **John Veroneau** | +1 202 662 5034 | jveroneau@cov.com |
| **Susan Cassidy** | +1 202 662 5348 | scassidy@cov.com |
| **Ashden Fein** | +1 202 662 5116 | afein@cov.com |
| **Heather Finstuen** | +1 202 662 5823 | hfinstuen@cov.com |
| **Zach Mears** | +1 202 662 6000 | zmears@cov.com |
| **Samantha Clark** | +1 202 662 5492 | sclark@cov.com |
| **Brian Williams** | +1 202 662 5270 | bwilliams@cov.com |
| **Jonathan Wakely** | +1 202 662 5387 | jwakely@cov.com |
| **Ruchi Gill** | +1 202 662 5131 | rgill@cov.com |
| **Doron Hindin** | +1 202 662 5903 | dhindin@cov.com |
| **Jordan Hirsch** | +1 202 662 5032 | jhirsch@cov.com |