Davis Polk

President Biden amends restrictions on connected software applications linked to Chinese companies

June 14, 2021 | Client Update | 7-minute read

Executive Order 14034 sets out an updated policy framework to address the risk that connected software applications can be exploited by foreign adversaries. The Order directs the Secretary of Commerce to lead an interagency review of connected software applications, their associated risks and ways to protect U.S. persons from such risks, and rescinds three of President Trump's executive orders that had authorized restrictions on use of specific software applications.

For the second time this month, the Biden administration has put its own stamp on China-related sanctions put into place by its predecessor. On June 9, 2021, the President issued Executive Order 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries" (EO 14034 or the Order), which sets out an updated policy framework to address the risk that connected software applications can be exploited by foreign adversaries to obtain access to sensitive personal and commercial data of U.S. persons. Most significantly, EO 14034 rescinds three of President Trump's executive orders—EOs 13942, 13943, and 13971—which authorized the Commerce Department to prohibit transactions involving TikTok, WeChat, and eight other communications and financial technology software applications.

Rather than targeting specific companies or applications, EO 14034 directs the Commerce Department to use existing authorities under another Trump administration executive order, EO 13873, to review and mitigate national security risks of transactions involving "connected software applications" [1] that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary. The Order also tasks two interagency reviews to further assess risks related to connected software applications, and provide recommendations for any additional authorities needed to address those risks.

We provide below a brief overview of the Trump administration initiatives affected by EO 14034, as well as a summary of the changes to those initiatives resulting from the Order.

Background

On May 15, 2019, then-President Trump issued EO 13873, "Securing the Information and Communications Technology and Services Supply Chain," which declared a national emergency arising from the acquisition and use in the U.S. of information and communications technology and services (ITCS) supplied by "foreign adversaries" and authorized the U.S. Department of Commerce to issue regulations that would prohibit U.S. persons from acquiring ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary."[2] On January 19, 2021, the U.S. Department of Commerce published an interim final rule implementing EO 13873 that, effective March 22, 2021, authorized the Department to prohibit or otherwise restrict U.S. transactions involving the ITCS supply chain that have a nexus with "foreign adversaries," which the Commerce Department has determined to include China.

Relying on the national emergency declared in EO 13873, and in response to concerns about collection of or access to sensitive personal data through certain mobile applications, the Trump Administration issued EOs 13942, 13943 and 13971, which, respectively, authorized the Commerce Department to prohibit U.S. persons from engaging in transactions involving TikTok, WeChat and WeChat Pay, and eight other Chinese-linked communications and financial technology software applications. These orders became the subject of substantial public controversy as a result of the popularity and wide usage of certain of the identified software applications, and EOs 13942 and 13943 were the subject of court challenges. Ultimately, none of the orders were actually implemented, as injunctions prevented the Commerce Department from enforcing prohibitions issued under EOs 13942 and 13943, and the Biden administration elected not to move forward with implementation of EO 13971.

Overview of EO 14034

EO 14034 accomplishes three functions. It revokes the three Trump administration executive orders described above, sets up a framework for the interagency to review threats relating to foreign adversaries' access to sensitive data and connected software applications and make additional policy recommendations, and provides additional direction to the Commerce Department concerning its implementation of EO 13873. We address each of these elements of the order in turn below.

Revocation of prior Executive Orders

Section 1 of EO 14034 revokes EOs 13942, 13943 and 13971 in their respective entireties. Section 2(a) instructs the Director of the Office of Management and Budget, as well as the heads of executive departments and agencies, to take steps to rescind any actions implementing or enforcing the aforementioned revoked Executive Orders. Moreover, all personnel positions, committees, task forces, or other entities established pursuant to EOs 13942, 13943 or 13971 are to be abolished.

While the revocation of three sanctions executive orders on its face appears to be a dramatic step, it is important to note that none of the orders had actually been implemented and their revocation thus does not change U.S. persons' legal obligations. Revocation of EOs 13942 and 13943 should resolve pending legislation challenging those orders, which had resulted in injunctions barring their implementation.

Interagency review

Under Section 2(b) of the Order, the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, and the heads of other agencies as the Secretary of Commerce deems appropriate (together, the Supporting Agencies), must issue a report to the National Security Advisor with recommendations to protect against (i) harm from the unrestricted sale of, transfer of, or access to U.S. persons' sensitive data,[3] and (ii) harm from access to large data repositories by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary. The report must be issued no later than 120 days after the effective date of EO 14034.[4]

Under Section 2(c) of the Order, the Secretary of Commerce, in consultation with the Supporting Agencies, must issue, within 180 days of the effective date of EO 14034, a report recommending additional executive and legislative actions to address the risks associated with connected software applications affiliated with foreign adversaries.

Implementation of EO 13873

Section 2(d) of the Order directs the Secretary of Commerce to evaluate, on a continuing basis, transactions involving connected software applications that may pose an undue risk of (i) the sabotage or subversion of ICTS in the U.S., (ii) catastrophic effects on the security or resiliency of the critical infrastructure or digital economy of the U.S., or (iii) catastrophic effects on the security or resiliency of the critical infrastructure or digital economy of the U.S. Based on these evaluations, the Secretary of Commerce must take appropriate action pursuant to EO 13873 and its implementing regulations.

Looking forward

As was the case with its reset of sanctions targeting U.S. investment in companies linked to China's military, which we discuss here, the issuance of EO 14034 shows that the Biden administration shares many of the policy concerns underlying Trump administration actions targeting China, as well as a continued willingness to leverage sanctions authorities to address those concerns. However, the Biden administration approach to utilizing such authorities appears to be more deliberative and targeted, and designed to put China-related sanctions programs on a stronger and more sustainable legal footing. Indeed, the White House stated that the intent of the order was to direct the use of a "criteria-based decision framework and rigorous, evidence-based analysis" to address the risks posed by ICTS transactions involving software applications linked to a "foreign adversary, including the People's Republic of China, that may present an undue or unacceptable risk to the national security of the United States and the American people."

EO 14304 comes on the heels of the Department of Commerce's recent announcement of a subpoena on a Chinese company to support the review of transactions pursuant to EO 13873. The Biden administration's decision to retain and increase reliance on that review process, as well as to task the interagency to develop recommendations for additional authorities in this space, shows a continued focus on addressing what the U.S. government perceives to be a significant Chinese threat to the U.S. ICTS supply chain and Americans' personal data. While TikTok influencers can now rest easy, U.S. companies and investors should continue to be mindful of both the current and future risks of engaging in transactions with entities that are involved in the U.S. ICTS supply chain and located in countries identified as foreign adversaries.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Kendall Howell
+1 202 962 7068
kendall.howell@davispolk.com

John B. Reynolds III
+1 202 962 7143
john.reynolds@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

[1] Section 3 of EO 14034 defines "connected software application" as "software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the internet."

[2] Our client update on EO 13873 can be found here.

[3] Sensitive data includes personally identifiable information, personal health information, and genetic information.

[4] No later than 60 days after the effective date of EO 14034, the Director of National Intelligence must provide threat assessments, and the Secretary of Homeland Security must provide vulnerability assessments, to the Secretary of Commerce to support development of the report required by Section 2(b).