International Trade Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Biden Issues Executive Order Redirecting and Clarifying Scrutiny of Chinese Apps

June 22, 2021

Key Points

- On June 9, President Biden signed an executive order ("EO") revoking a series of Trump-era EOs targeting specific Chinese "connected software applications" ("apps"), including TikTok and WeChat.
- The EO calls for a "rigorous, evidence-based analysis" of potential risks posed by apps designed, developed, manufactured or supplied by China and other "foreign adversaries" and identifies the Information and Communication Technology and Services ("ICTS") Supply Chain EO and its implementing regulations (15 C.F.R. Part 7) as the primary tool for addressing the national security risks posed by such apps and other ICTS products and services.
- The EO establishes app-specific factors that should be evaluated as part of the Department of Commerce's review under the ICTS Supply Chain regulations to determine whether certain apps present national security concerns.
- This action, along with the redesign of the Chinese investment sanctions program (discussed more fully in our client alert here), demonstrates that the Biden-Harris administration acknowledges many of the same national security risks identified by the prior administration, but is opting to address those risks through a fact-based regulatory assessment of specific cases based on a defined criteria.

Background

On June 9, 2021, President Biden issued Executive Order 14034 (Protecting Americans' Sensitive Data from Foreign Adversaries) ("EO 14034") to revoke the three Trump administration "app ban" EOs that targeted TikTok, WeChat and eight other Chinese applications:

I. Executive Order 13942 of August 6, 2020 (Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain) ("TikTok App Ban EO");

II. Executive Order 13943 of August 6, 2020 (Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With

Contact Information

If you have any questions concerning this alert, please contact:

Christian C. Davis
Partner
chdavis@akingump.com
Washington, D.C.
+1 202.887.4529

Shiva Aminian
Partner
saminian@akingump.com
Los Angeles
+1 310.552.6476

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

David C. Vondle
Partner
dvondle@akingump.com
Washington, D.C.
+1 202.887.4184

Clete R. Willems
Partner
cwillems@akingump.com
Washington, D.C.
+1 202.887.4125

Katherine P. Padgett
Counsel
kpadgett@akingump.com
Washington, D.C.
+1 202.887.4079

Respect to the Information and Communications Technology and Services Supply Chain) ("WeChat App Ban EO"); and

III. Executive Order 13971 of January 5, 2021 (Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies) ("EO 13971").

This EO arose in the context of legal setbacks that the U.S. government had faced in lawsuits brought by TikTok and the users of TikTok and WeChat and is the second time in a month that the Biden-Harris administration has modified or replaced Trump administration EOs to address court challenges.[1] In this instance, the courts had issued preliminary injunctions derailing the Department of Commerce's efforts to implement the TikTok and WeChat App Ban EOs last year, which had halted any enforcement of those orders. Although the Trump administration had appealed those preliminary injunction rulings, in February, following President Biden's inauguration, the Department of Justice ("DOJ") moved to have those appeals held in abeyance pending further review by incoming Biden-Harris administration officials.

Under EO 14034, U.S. government agencies are to (i) rescind "any orders, rules, regulations, guidelines or policies implementing or enforcing" those EOs and (ii) abolish "any personnel positions, committees, task forces, or other entities" established pursuant to those EOs. On June 21, the Commerce Department submitted a Federal Register notice, and confirmed on its website, that consistent with EO 14034 the Secretary of Commerce has rescinded the two Commerce actions issued under the now-revoked TikTok and WeChat App Ban EOs. In filings made on June 11, the DOJ informed the relevant appellate courts that it believes those anticipated rescissions "affect whether a live controversy remains" in the pending appeals and that it expects to submit dispositive motions by July 12, 2021.

New Approach

EO 14034 reaffirms that apps designed, developed, manufactured or supplied by "foreign adversaries" may present national security concerns, particularly in relation to the collection of user data, and requires a further examination of those potential concerns. It further reaffirms the Trump administration's declaration of a national emergency with respects to the ICTS supply chain from May 15, 2019. Rather than direct specific action against identified apps on a mandated timeline, however, the EO directs any further consideration of the risks posed by such apps to the Secretary of Commerce under the ICTS Supply Chain EO and its implementing regulations (15 C.F.R. Part 7) and leaves it within the Secretary's discretion to take appropriate action to mitigate any unacceptable or undue risks using that authority.[2] Please see further below for a summary of those ICTS Supply Chain regulations and our previous client alert for a more in-depth discussion of that new rule.

EO 14034 underscores that any assessment of the threats to U.S. national security posed by apps will be evaluated using a "**rigorous, evidence-based analysis**" and that any unacceptable or undue risks should be addressed consistent with "the preservation and demonstration of America's core values and fundamental freedoms."

Evaluations of the risk posed by any particular app under the ICTS Supply Chain regulations must consider the following factors, in addition to the criteria set forth in those regulations:

- Ownership, control or management by persons that support a foreign adversary's military, intelligence or proliferation activities.
- Use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data.
- Ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary.
- Ownership, control, or management of connected software applications by persons involved in malicious cyber activities.
- A lack of thorough and reliable third-party auditing of connected software applications.
- The scope and sensitivity of the data collected.
- The number and sensitivity of the users of the connected software application.
- The extent to which identified risks have been or can be addressed by independently verifiable measures.

The EO does not impose a timeline for assessing the national security concerns presented by specific apps or for imposing any prohibitions against those apps. We expect, however, that any subsequent action under the ICTS Supply Chain regulations will be informed by the reports and assessments ordered by President Biden under EO 14034. The EO directs the Secretary of Commerce, in consultation with relevant U.S. government agencies, to provide two reports to the National Security Advisor. First, within 120 days, a report recommending actions to protect against (i) "harm from the unrestricted sale of, transfer of, or access to United States persons' sensitive data, including personally identifiable information, personal health information, and genetic information," 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." These recommendations are expected to be based, in part, on threat and vulnerability assessments produced within 60 days by the Director of National Intelligence and the Secretary of Homeland Security, respectively. Second, within 180 days, a report recommending additional executive and legislative actions related to the risk posed by "connected software applications" that are "designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary."

Overview of ICTS Supply Chain EO and Implementing Regulations

As directed by the EO, the Commerce Department is to consider any risks posed by apps designed, developed, manufactured or supplied by China and other "foreign adversaries" under the new ICTS Supply Chain EO and its implementing regulations. In effect since March 22, 2021, those implementing regulations authorize the Secretary of Commerce to identify, mitigate, prohibit and/or unwind (i) covered "ICTS Transactions" (ii) that involve "ICTS designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a 'foreign adversary'" and (iii) that pose an undue or unacceptable risk.

Scope: The ICTS Supply Chain regulations cover "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications

technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download" involving ICTS technologies, hardware or software in one of the following six categories:

IV. **Critical Infrastructure** as defined by Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience.

V. **Networking**: Wireless local area networks; Mobile networks; Satellite payloads; Satellite operations and control; Cable access points; Wireline access points; Core networking systems; and Long- and short-haul networks.

VI. **Hosting and Storage of Sensitive Personal Data**: Internet hosting services; Cloud-based or distributed computing and data storage; Managed services; and Content delivery services.

VII. **Widely Sold Surveillance, Monitoring or Networking Devices**: Internet-enabled sensors, webcams and any other end-point surveillance or monitoring device; Routers, modems, and any other home networking device; or Drones or any other unmanned aerial system.

VIII. **Widely Used Internet Communications Software Applications**: Desktop applications; Mobile applications; Gaming applications; and Web-based applications.

IX. **Emerging Technologies**: Artificial intelligence and machine learning; Quantum key distribution; Quantum computing; Drones; Autonomous systems; or Advanced Robotics.

Foreign Adversary: The ICTS Supply Chain regulations designate the following six countries and regimes as "foreign adversaries": China (including Hong Kong), Cuba, Iran, North Korea, Russia and the Maduro regime in Venezuela.

Undue or Unacceptable Risk: An ICTS transaction will be considered to pose an "undue or unacceptable risk" if the Secretary of Commerce assesses that it creates (i) an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICTS in the United States; (ii) an undue risk of catastrophic effects on the security or resiliency of U.S. critical infrastructure or the U.S. digital economy; or (iii) an unacceptable risk to U.S. national security or the security and safety of U.S. persons.

Looking Ahead

By redirecting the assessment and mitigation of any threats to national security posed by apps designed, developed, manufactured or supplied by "foreign adversaries" to the ICTS Supply Chain EO and its implementing regulations, EO 14034 offers a further example of how the Biden-Harris administration intends to address national security risks associated with China. While largely acknowledging the various underlying national security concerns that the prior administration sought to address—here, the risks posed by the collection of vast swathes of U.S. citizens' sensitive personal data by mobile apps—the Biden-Harris administration is opting to assess and address those threats using fact-based analyses of specific cases based on a defined criteria.

Finally, EO 14034's focus on the risks posed by access to proprietary business information forecasts a possible increase in trade secret misappropriation claims or similar actions against foreign companies.

[1] On June 3, 2021, President Biden issued Executive Order 14032 that revoked the Trump administration's investment ban on "Communist Chinese Military Companies" and replaced it with a similar "Chinese Military-Industrial Complex Companies" (CMIC) sanctions program. For a more detailed discussion of that EO, please see our previous client alert here.

[2] With respect to the specific risks to U.S. national security, the EO identifies the "increased use" in the United States of "connected software applications" that are "designed, developed, manufactured, or supplied" by persons subject to the jurisdiction of the People's Republic of China and the other foreign adversaries identified in the ICTS Supply Chain regulations. The EO states that risk is based on the capabilities of such "connected software applications" to "access and capture vast swaths of information from users, including United States persons' personal information and proprietary business information" and in turn facilitate or provide access to foreign adversaries seeking to steal or obtain that data.

akingump.com