New E.O. Revokes TikTok and WeChat Prohibitions, But Lays Framework for New Restrictions

June 10, 2021

Yesterday, President Biden signed an Executive Order ("E.O.") that formally revokes and replaces three earlier E.O.s that aimed to restrict transactions with TikTok, WeChat, and other communications and Fintech applications and provides a new framework to address security concerns related to the information and communications technology and services ("ICTS") supply chain. The new E.O. was issued pursuant to the ongoing national emergency declared in the 2019 E.O. 13873 regarding ICTS in the United States that are controlled by persons within the jurisdiction of a "foreign adversary," including China.

The new E.O. resets the U.S. government's approach to ICTS by ordering a review of the national security threats posed by software applications that collect Americans' sensitive personal and business data and by foreign adversaries' access to large repositories of U.S. person data. New restrictions are likely following that review, and companies that rely on software applications owned or managed by companies linked to China or other potential foreign adversaries, should closely watch developments in this space.

New reports on "unacceptable or undue risks" posed by foreign adversary-connected applications

The E.O. directs the Directors of National Intelligence and Homeland Security to provide threat and vulnerability assessments to the Secretary of Commerce. In turn, the Commerce Department will draft two reports on foreign adversary-connected software, defined as software that has the ability to collect, process, or transmit data over the internet. The reports will recommend actions to protect against harm from the sale of, transfer of, or access to U.S. persons' sensitive data, including personally identifiable information, personal health information, and genetic information. In addition, the Commerce Department will recommend additional actions to address risks associated with 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.

Several criteria indicate national security risk of ICTS applications

Building on the criteria to assess national security threats listed in E.O. 13873, the new E.O. lists several factors that will be considered when evaluating the risks posed by foreign adversary-connected software, including:

- ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities;

- use of the connected software applications 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; and
- the extent to which identified risks have been or can be addressed by independently verifiable measures.

Consistent with other recent Biden Administration actions targeting China, the E.O. notes that the U.S. government may impose consequences on non-U.S. persons who own, control, or manage connected software applications that engage in serious human rights abuse or otherwise facilitate such abuse.

These criteria will inform the U.S. government's decision-making framework to adopt a "rigorous, evidence-based" analysis to address risks posed by ICTS transactions involving foreign adversary-connected software.

Further action on ICTS applications likely

Although yesterday's E.O. rescinds the previous E.O.s dealing with Chinese mobile applications, new restrictions on Chinese and other software that collect large amounts of sensitive U.S. person data are likely to flow from the Commerce Department's forthcoming report and recommendations, which are expected within 180 days. Furthermore, the E.O. provides the Commerce Department with authority to restrict transactions and business activities that may:

- Pose a risk of sabotage or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICTS in the United States;
- Pose a risk of catastrophic effects on the security or resiliency of the critical infrastructure or digital economy of the United States; or
- Otherwise pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.

Our Export Controls and Sanctions team will be actively monitoring for any developments.