SOURCEREE

NATIONAL SECURITY NEWSLETTER

OCTOBER 2022

- President Biden issued a new Executive Order (E.O.) titled, “Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States.”
- Team Telecom Two-Year Anniversary
- TikTok Seen Moving Toward U.S. Security Deal, but Hurdles Remain
- US Treasury Department Derails Asymchem's Acquisition of Snapdragon

October 2022 Newsletter

National Security Investment Reviews

Issue 1: President Biden issued a new Executive Order (E.O.) titled, "Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States."

Source: https://www.winston.com/en/global-trade-and-foreign-policy-insights/winstons-thoughts-on-president-bidens-new-cfius-executive-order.html

Considerations:
This is the first E.O. since CFIUS was established in 1975 to provide presidential direction on the factors that CFIUS is required to consider when evaluating foreign investments in U.S. businesses. Specifically, the E.O. states that CFIUS is required to consider the following four factors when evaluating transactions: (1) the transaction's effect on supply chain resilience and security, both within and outside of the defense industrial base; (2) the transaction's effect on U.S. technological leadership in areas affecting U.S. national security; (3) cybersecurity risks that may impair national security; and (4) risk to U.S. persons' sensitive data. The E.O. also clarifies that if a foreign person has made multiple investments in an industry or sector, CFIUS will not look at each new investment in a vacuum, but rather will consider the cumulative effect of all of a foreign person's investments in a particular industry or sector when evaluating the national security risks arising from each new investment. Finally, the E.O. requires CFIUS to provide regular reports to the White House's National Security Advisor regarding its regulations, processes, and procedures.

The Executive Order May Give CFIUS Member Agencies a Basis to Mitigate/Block Risks Based on (Highly) Speculative Risk Assessments

When considering technology transfer risks, the E.O. states that the Committee shall consider whether a transaction could result in "future advancements and applications" in technology that could undermine national security. The E.O. also states that the Committee is required to consider third-party ties that "might" cause the transaction to impair the national security of the United States. Moreover, when considering data risks, the E.O. notes that it is important for the Committee to consider "potential risks" posed by foreign persons who "might" exploit access to certain data on U.S. persons. There has always been debate within the Committee about how speculative a risk assessment can be and still serve as a basis for mitigating or blocking a transaction, and it is too early to know how the Committee will interpret the E.O. But member agencies may try to use some of the E.O.'s broad language as a basis to mitigate or block transactions based on risk assessments about what foreign companies might do in the future, even if those risk assessments are (highly) speculative.

Issue 2: Team Telecom Two-Year Anniversary

Source: https://www.whitecase.com/insight-alert/team-telecom-two-year-anniversary

Considerations:
On April 4, 2020, the President signed Executive Order 13913 (the EO), "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," formalizing Team Telecom (or "the Committee"). Pursuant to the EO, the Committee's primary objective is to assist the FCC in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications sector.

As indicated in our April 2020 client alert following the EO, we expected increased scrutiny by the Committee of Chinese involvement in the US telecommunications sector. Since that time, the FCC, upon the advice and guidance of Team Telecom, has revoked various telecommunications licenses held by Chinese entities. We expect this heavy scrutiny—which has persisted during both the previous and current presidential administrations—to continue.

Consistent with this trend and the EO's express directive, we also expect Team Telecom to be more aggressive in reviewing existing licenses. In doing so, Team Telecom will apply its more robust procedures, including better coordination among Committee Members, Committee Advisors, and the Intelligence Community, which may not have been consulted when the licenses were first granted under Team Telecom's less formal approach pre-EO. This is also consistent with the FCC's interest in coordinating with the Executive Branch on implementing periodic reviews of foreign carriers' authorizations to "stay on top of evolving national security, law enforcement, policy, and trade risks." Unlike in the Committee on Foreign Investment in the United States ("CFIUS"), which provides a safe harbor (absent limited circumstances) to transactions that have cleared CFIUS's review, the FCC may revoke previously granted licenses. As the geopolitical climate becomes more uncertain, and as the Executive Branch's national security and law enforcement interests become more aggressive, we expect increased imposition of mitigation for, and revocation of, existing licenses held by foreign carriers.

For similar reasons, we expect the FCC, in consultation with Team Telecom, to more carefully scrutinize submarine cable landing licenses and more selectively grant special temporary authority related to such licenses. As the FCC noted in its China Telecom order, "[f]or too long, it was the practice of [the FCC] to unilaterally grant applicants special temporary authority to start building submarine cables while their applications were pending, even if those applications reflected ownership by state-owned companies that could represent a national security risk. That's no longer the case. Requests for special temporary authority to start construction can raise national security concerns too, and the FCC now sends such requests to [Team Telecom] for coordinated security review."

Issue 3: TikTok Seen Moving Toward U.S. Security Deal, but Hurdles Remain

Source: https://www.nytimes.com/2022/09/26/technology/tiktok-national-security-china.html

Considerations:
The Justice Department is leading the negotiations with TikTok, and its No. 2 official, Lisa Monaco, has concerns that the terms are not tough enough on China, two people with knowledge of the matter said. Completing an agreement may also be difficult at a tricky political moment for the Biden administration, which has stepped up its cadence of criticism and executive actions addressing China. The policy toward Beijing, while expressed in more diplomatic language, is not substantially different from the posture of the Trump White House, reflecting a suspicion of China that now spans the political spectrum.

TikTok has been negotiating with representatives for the Committee on Foreign Investment in the United States, or CFIUS, a group of federal agencies that reviews investments by foreign entities in American companies, to resolve concerns that the app puts national security at risk. The group would need to sign off on an agreement, and potentially President Biden as well.

TikTok declined to comment on the talks but said it was "confident" that it was "on a path to fully satisfy all reasonable U.S. national security concerns."

Negotiations between CFIUS and TikTok have dragged on as officials wrapped their arms around complex technical questions about the app. They edged closer to a detailed agreement in recent months, two people with knowledge of the discussions said. Under the draft terms, TikTok would make changes to three main areas, the people with knowledge of the discussions said.

- First, TikTok would store its American data solely on servers in the United States, probably run by Oracle, instead of on its own servers in Singapore and Virginia, two of the people said.

- Second, Oracle is expected to monitor TikTok's powerful algorithms that determine the content that the app recommends, in response to concerns that the Chinese government could use its feed as a way to influence the American public, they said.

- Lastly, TikTok would create a board of security experts, reporting to the government, to oversee its U.S. operations, three people with knowledge said.

Issue 4: US Treasury Department derails Asymchem's acquisition of Snapdragon

Source: https://cen.acs.org/business/investment/US-Treasury-Department-derails-Asymchem-acquisition-of-Snapdragon/100/web/2022/09

Considerations:
Snapdragon Chemistry, a drug services firm specializing in flow chemistry technology, says its acquisition by Asymchem, a pharmaceutical research and manufacturing company based in China, will not proceed. The deal was first announced in February.

It fell through as Snapdragon and Asymchem were unable to settle on mitigation terms that would satisfy the US Treasury's Committee on Foreign Investment in the United States (CFIUS).

Snapdragon manufactures early- and clinical-stage drug candidates in volumes of up to about 30 kg, and the acquisition would have provided access to later-stage and commercial-scale production at Asymchem's plant in Tianjin, China, according to Snapdragon CEO Matt Bio. Conversely, the deal would have given the Chinese company early-stage manufacturing assets in the crucial US market.

Snapdragon was formed in 2014 as a spin-out from the Massachusetts Institute of Technology.

It received $700,000 from the US Biomedical Advanced Research and Development Authority in 2020 to develop a continuous process for nucleotide triphosphates used to produce messenger RNA vaccines.

The company has worked in partnership with Asymchem in recent years, and the Chinese firm participated in an $8.5 million investment round in 2020 allowing Snapdragon to build its first pharmaceutical production suites. The company recently commissioned a 4,700 m2 research and manufacturing facility in Waltham, Massachusetts.

Snapdragon CEO Matt Bio says parties to the acquisition did not anticipate a government challenge, given other deals in the sector involving Chinese companies, notably Porton's purchase of a similar firm, J-Star Research, in 2017.

"As the political climate deteriorated since February, it did appear that it might be a challenge to get approval," Bio says. "We will continue our growth plans. We have access to capital. It was just a lot of wasted time at this point."

Snapdragon plans to continue working with Asymchem at customers' discretion, Bio says.

Issue 5: House passes telecom security measures on untrusted equipment, global approaches

Source: https://insidecybersecurity.com/daily-news/house-passes-telecom-security-measures-untrusted-equipment-global-approaches

Considerations: Countering Untrusted Telecommunications Abroad Act

The House, in September 2022, approved two bills addressing telecommunications system security, with one requiring reports on use of untrusted equipment by allies and at U.S. embassies, and the second requiring development of a global strategy in support of secure telecom infrastructure.

H.R. 8520, the "Countering Untrusted Telecommunications Abroad Act," cites threats posed by Chinese firms Huawei and ZTE and calls for a report from the Secretary of State within six months on "the prevalence of untrusted telecommunications equipment or services in the networks of United States allies and partners."

The bill requires details such as "an enumeration of any mobile carriers that are using the untrusted telecommunications equipment or service present, and any mobile carriers that are not," and "a determination of whether the untrusted telecommunications equipment or service present is in the core or periphery of the network," as well as plans to "rip and replace the untrusted telecommunications equipment or service present with a trusted telecommunications equipment or service."

Considerations: FCC's Rosenworcel identifies funding shortfall for Huawei rip-and-replace program; industry urges Congress to act

The FCC will need approximately $3 billion to fund reimbursement requests under the rip-and-replace program designed to rid mostly rural telecom systems of equipment made by Chinese companies Huawei, ZTE and others that has been determined by the U.S. government to raise unacceptable national security risks.

"To fund all reasonable and supported cost estimates within the first and third prioritization groups and cover administrative expenses, the Reimbursement Program will require $4.98 billion, reflecting a current shortfall of $3.08 billion. There are no applications that fall within the second prioritization category," Rosenworcel said.

She said, "Absent an additional appropriation, the Commission will apply the prioritization scheme Congress specified in the [fiscal 2021 Consolidated Appropriations Act]. Because demand within the first prioritization group exceeds available funds for the Reimbursement Program, the Commission will prorate reimbursement funds equally to each eligible applicant in the first prioritization group. The pro-rata factor for those allocations will be approximately 39.5% of demand."

Protected by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.

- Software platform for on-demand supply chain risk assessments and financial intelligence data
- Analytical Support
- Business intelligence reports on critical suppliers