GDR NEWS

US strengthens data-rich inbound investment rules

Sam Clark

Proposed rule changes would allow the US foreign investment committee to block deals that might endanger sensitive personal data.

The US Department of the Treasury yesterday issued proposed regulations to implement the Foreign Investment Risk Review Modernization Act (FIRRMA). The regulations would give the Committee on Foreign Investment in the United States (CFIUS) jurisdiction to investigate and block a wider range of transactions, with a view to letting it better address national security concerns.

The proposed regulations would empower the committee to investigate and block foreign investment into US businesses that are involved in critical technology and infrastructure, or that handle sensitive personal data.

First published on the *Global Data Review* website, 19 September 2019

The changes also hand CFIUS the right to consider new factors in its assessment of national security risks, including the extent to which a transaction is likely to expose personally identifiable information, genetic information, or other sensitive data of US citizens to access by a "foreign government or foreign person that may exploit that information in a manner that threatens national security".

Under the new rules, the committee would also be able to consider whether a transaction might create cybersecurity vulnerabilities in the US.

The regulations additionally propose a change to the threshold that triggers CFIUS's involvement. Companies would be required to notify the committee about investments that give a foreign actor any decision-making power, or access to private information or sensitive data. The existing regime currently only lets the committee investigate investments that give foreign entities full control over US businesses.

If passed, the rule changes will require the US secretary of commerce to provide a report to Congress and CFIUS about investment made by Chinese companies every two years. That report will have to include breakdowns of investment by Chinese companies based on value and other factors.

Blackmail threat

Observers said that the proposed changes could greatly increase the level of due diligence involved in transactions.

Richard Sofield, a partner at Wiley Rein in Washington, DC, said the changes would be a "significant adjustment".

"They would result in a longer timeline for deals to get done, and a greater cost as companies have to expand their due diligence," Sofield said.

He noted that to fall under the CFIUS's jurisdiction, companies must hold data that either relates to genetic information, government staff or more than a million citizens. To qualify, data must also fall into certain categories.

The categories, Sofield said, reflect the government's concerns about foreign investment and national security. One category includes information about individuals' financial distress or hardship. "That makes them a target for economic espionage – paying people to steal technology", Sofield said.

First published on the *Global Data Review* website, 19 September 2019

The changes would also cover data regarding health insurance and professional liability insurance. “Insurance is a goldmine for a threat actor – they have a lot of information, including job history for professional liability insurance. That’s potential blackmail material if you’ve been involved in any misconduct,” he said. Biometric data is also included, as it has “potential for espionage and identity fraud”, Sofield said.

The committee rarely gets as far as making a recommendation to the president to block a transaction, Sofield said. Instead, companies more often abandon transactions before that point – a practice that is likely to increase given the committee’s new powers, he said.

It is also common for the committee to negotiate specific terms with companies, Sofield said. That could include prohibiting access to sensitive personal data by the foreign entity or a requirement to build certain security systems. These types of agreement are “far more common” than an outright block, Sofield said.

Giovanna Cinelli, a partner at Morgan Lewis & Bockius in Washington, DC, told GDR that if the rules are implemented as they are, there is likely to be “some confusion about what is actually a covered transaction as parties manage and interpret the new definitions and exceptions”.

However, Cinelli said, the CFIUS has a history of laying down broad rules and definitions and gradually “softening” requirements through implementation and certain exceptions – for instance for certain types of transactions and for investment from certain countries.

The proposed data changes are likely to cause most difficulties for companies in industries that have not previously been under the CFIUS’s jurisdiction but may be caught by the new rules. “Health and property insurers, for instance, understand privacy violations, identity theft and so on, but haven’t traditionally played in this space. I expect some comments from them,” Cinelli said.

There is also likely to be some “reservation” about the broad rules that apply to transactions or investments that involve genetic information, Cinelli said, given how many startups and universities – who are unlikely to be used to this type of regulation – develop that type of data.

Scott Boylan, a senior adviser at consultancy StoneTurn in Washington, DC, said that the proposed regulations should ease companies’ fears. “There was a lot of concern when the law originally came out, because it’s a very broad provision. People thought that basically anyone with an HR department would get caught. The regulations make it a lot better and a lot more focused,” he said.

First published on the *Global Data Review* website, 19 September 2019

The aim of the rules is to protect government intelligence officials, Boylan said. “The government is primarily concerned with foreign entities collecting information from acquisitions that they can use to identify government personnel, in particular intelligence officers – that’s the top concern.”.

Boylan noted that it is “absolutely” likely that CFIUS could force companies to store US citizens’ data on US soil. The committee also has the power to mandate that companies operate separate IT systems to protect US data from foreign investors, he said.

However, it is likely that the committee will draw up a “good countries list”, Boylan said, which will dictate which jurisdictions it believes present less of a risk. “I’d be shocked if the UK wasn’t one of the first on that list,” he said.

Stephen Heifetz, a partner at Wilson Sonsini Goodrich & Rosati in Washington, DC, said that the complexity of the definitions of critical technology, critical infrastructure, or sensitive personal data means that “there is a high likelihood of CFIUS being able to exercise jurisdiction if it chooses to do so”.

The proposed changes are open for comments until 17 October. The rules, in their eventual version, will take effect no later than 13 February 2020.

First published on the *Global Data Review* website, 19 September 2019