Insurance Sector Should Expect More Focus From CFIUS

By **Nicholas Klein, Gabriel Gershowitz and Prakash Paran** (September 9, 2020)

Nicholas Klein

Gabriel Gershowitz

Prakash Paran

The U.S. government continues to take significant steps to address risks to national security posed by foreign geopolitical adversaries. One of the more prominent of these measures is the expansion of national security reviews of inbound acquisitions and investment by the Committee on Foreign Investment in the United States.

CFIUS is the U.S. government committee charged with identifying, evaluating and mitigating national security threats posed by foreign investment. It may be surprising to learn that the U.S. government considers insurance companies likely to present national security risks, and that transactions in the insurance sector are squarely in the crosshairs of CFIUS jurisdiction.

The fact is, as described in this article, insurance sector professionals should be aware of CFIUS risk to their transactions, particularly because of the U.S. government's demonstrated national security focus on transactions involving any of the following:

- Sensitive data on U.S. persons;
- Critical technology, including certain software and research and development activities, and
- Important U.S. infrastructure or real estate.

The U.S. government's recent increased scrutiny of transactions involving these potential national security risks has significant implications for the insurance industry. Indeed, several insurance-related transactions have faced CFIUS scrutiny and been forced to accept CFIUS conditions to complete transactions in recent years.[1]

New regulations promulgated under the Foreign Investment Risk Review Modernization Act are intended to address these concerns by strengthening the authority of CFIUS to review a wider variety of investments. Effective Feb. 13, these regulations expand CFIUS' jurisdiction to review certain noncontrolling investments in U.S. businesses and a broad range of real estate transactions.

This article outlines the scope of CFIUS jurisdiction in light of the recent changes to the CFIUS regime and presents some critical CFIUS considerations for the insurance sector.

CFIUS Has Broad Powers to Review Mergers, Acquisitions and Other Investments

CFIUS is an interagency committee chaired by the U.S. Department of the Treasury with

representatives from several executive branch agencies. CFIUS has jurisdiction over covered control transactions, i.e., transactions that could result in foreign control of a U.S. business, each as defined by regulation; noncontrolling investments in certain types of U.S. businesses; and certain real estate transactions.

CFIUS has authority to review such transactions, and where an investment may present a threat to U.S. national security, the president — upon CFIUS' recommendation — can block or impose conditions on the investment to mitigate the perceived threat, such as by limiting the foreign investor's access to technical information or data of the U.S. target business.

Until the launch of the critical technology pilot program in November 2018 and the recent, expansive regulations mentioned above, CFIUS had been an entirely voluntary process whereby the parties to a transaction could receive the benefit of a safe harbor from the risk of future CFIUS review and intervention.

CFIUS has authority to review completed transactions that it has not already reviewed, going as far back as 1988, although to review transactions completed more than three years ago requires chairperson approval. Indeed, in recent months, CFIUS has sought to review non-notified transactions completed as far back as 2011, and possibly even earlier.

Thus, receiving CFIUS approval upon satisfaction that there are no unresolved national security concerns prior to closing a transaction provides a significant benefit: It eliminates the risk that CFIUS will later review and seek to mitigate the transaction by imposing restrictions on the foreign investor's access or control rights vis-à-vis the U.S. business, or potentially to require the foreign investor to divest its interest entirely.

There are two limited circumstances where parties are required to file with CFIUS: (1) the U.S. business produces, designs, tests, manufactures, fabricates or develops a critical technology for use in connection with one of 27 industries identified by North American Industry Classification System, or NAICS, code; or (2) certain transactions involving a direct or indirect investment by a foreign government.

On May 21, CFIUS introduced a proposed change to the mandatory filing requirement for transactions involving critical technology.[2] The change would replace the requirement that the critical technology is used in or specifically designed for use in specific industries identified by NAICS code with the requirement that the critical technology would require an export license to provide it to any of the foreign persons involved in the transaction.

CFIUS has the extraordinary authority to block a transaction outright — including by issuing a temporary stay while it evaluates a deal — or even to unwind a transaction by forcing the acquiror or investor to divest its interest under CFIUS' supervision. Failure to assess and account for this risk in an acquisition agreement also can lead to excessive costs in due diligence, extended interest payments in financing arrangements for the investor, and lost opportunities from other investors for the U.S. business.

Although not the focus of this article, the disposition of distressed assets, bankruptcy proceedings and convertible debt transactions, which may be seen more frequently due to the current macroeconomic environment, may be subject to CFIUS review.

Heightened National Security Concerns Over Collection of Data on U.S. Persons, Access to Critical Technology and Noncontrolling Investments

Although perhaps not intuitively thought of as involving national security concerns, the

insurance industry touches several CFIUS flashpoints — chief among them, access to sensitive personal data on U.S. persons and critical technologies. The recent expansion of CFIUS' jurisdiction has specifically targeted these areas, making it more likely that investments involving U.S. insurance sector companies will be subject to CFIUS review.

Indeed, CFIUS has actively sought to review transactions and required significant mitigation measures — including forced divestitures — for transactions involving personally identifiable information and personal health information on U.S. persons.[3]

The Foreign Investment Risk Review Modernization Act and its implementing regulations direct CFIUS to focus on industries and sectors that had not previously been considered to pose national security risks in the context of cross-border transactions. Among the types of U.S. businesses identified for heightened CFIUS scrutiny — known as TID U.S. businesses[4] — are U.S. businesses that collect or maintain certain types of sensitive personal data on U.S. persons. Explicitly included in the definition of sensitive personal data are:

- Insurance application information;
- Health information of individuals;
- Financial information that could be used to determine financial distress or hardship;
- Data from a consumer report, subject to certain exceptions;
- Nonpublic electronic communications such as email or text messaging;
- Biometric enrollment data;
- Information about U.S. government security clearances and applications for such clearances;
- Genetic information, such as genetic test results; and

- Geolocation data, regardless of the method of collection (e.g., mobile app, vehicle GPS, wearable).

A U.S. business is considered a TID U.S. business if it has a demonstrated business objective to maintain or collect identifiable data within one of the categories above on greater than one million U.S. persons, including customers and policyholders, but generally excluding the U.S. business's own employees, or it has done so at any point in the preceding 12 months.

It is important to note that a U.S. business will be considered a TID U.S. business if it collects or maintains any amount of genetic information or data from products targeted or tailored for U.S. national security agencies or their personnel and contractors (i.e., the one million individuals threshold does not apply). Note that publicly available information is generally not considered to be sensitive personal data.

As the insurance industry increasingly leverages technology in its business operations and targets technology companies as part of its investment strategy, the likelihood of triggering CFIUS jurisdiction because of critical technologies is more likely. Another type of TID U.S. business is one that produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies, defined to include a wide array of technology and software.

Access to these technologies by foreign adversaries is thought to threaten U.S. technological advancement and superiority in certain areas. As part of a broader effort to control technology transfer — one of the leading national security concerns of the U.S. government — CFIUS is intended to prevent foreign access to U.S.-developed technology through investment in or acquisition of U.S. businesses.

In addition to increased scrutiny and potentially more restrictive mitigation measures, transactions involving a TID U.S. business are now subject to expanded CFIUS jurisdiction to review. Historically, a transaction had to result in a foreign person gaining control of a U.S. business for CFIUS to have jurisdiction.

For TID U.S. businesses, however, the Foreign Investment Risk Review Modernization Act expanded CFIUS' jurisdiction to include review of noncontrolling investments if the investor also obtains certain rights vis-à-vis the U.S. business.

Specifically, CFIUS may review a noncontrolling, minority investment in a TID U.S. business completed or subject to a definitive agreement on or after Feb. 13 that affords a foreign person access to material nonpublic information, board or board observer rights, or substantive decision-making power with respect to certain aspects of the U.S. business's operations. These rule changes therefore make it more likely that investments in U.S. insurance sector companies will fall within CFIUS' jurisdiction.

CFIUS May Review Real Estate Investments

CFIUS also now has expanded jurisdiction to review real estate transactions.[5] As of February, CFIUS has authority to review transactions involving the purchase or lease by, or concession to, a foreign person — including real estate investment trusts — of certain real estate in the U.S.

Before the new regulations, CFIUS would have reviewed real estate involved in the investment in or acquisition of a U.S. business for proximity to sensitive locations. For

example, CFIUS has caused parties to abandon transactions involving the acquisition of an office building that housed sensitive tenants and the acquisition of a hotel because it was near a U.S. Navy training site.

These same concerns led to the recent expansion of authority to review real estate transactions that do not involve investment in a U.S. business, or so-called greenfield investments. Insurance companies should be aware of these changes, including if they own real estate within their investment portfolios or for their own occupancy.

The regulations contain numerous limitations and long lists of sensitive U.S. government or military sites. Foreign investments in real estate that otherwise seem innocuous may trigger CFIUS review if, for example, the real estate is within close proximity of certain sensitive locations or within an airport or maritime port. Parties to a transaction involving real estate, including the acquisition of distressed assets, should evaluate whether CFIUS might be an issue.

Conclusion

The insurance sector touches several national security flashpoints that are likely to raise CFIUS concerns, particularly in the current macroeconomic and nationalistic political environment. Given the high stakes of failure to account for CFIUS risks in transaction planning, and CFIUS' increased efforts to identify non-notified transactions, it is more important than ever for companies to conduct early due diligence to identify and understand their CFIUS exposure and to navigate the CFIUS process successfully.

Nicholas Klein and Gabriel Gershowitz are of counsel, and Prakash Paran is a partner, at DLA Piper.

[1] For example, in the China Oceanwide Holdings Group Co., Ltd, acquisition of Genworth Financial, Inc., CFIUS required that the parties arrange for a U.S.-based, third-party service provider to manage and protect the personal data of Genworth's U.S. policyholders to receive approval for the deal.

[2] CFIUS proposes export control-based reforms to its mandatory filing program (https://www.dlapiper.com/en/us/insights/publications/2020/05/cfius-proposes-export-control-based-reforms-to-its-mandatory-filing-program/).

[3] For example, CFIUS recently ordered the divestiture of Grindr (a software company that collects personal data including HIV status) and digital health company PatientsLikeMe.

[4] A "TID U.S. business" is named for the three categories of U.S. businesses included in its definition subject to several parameters: critical technology, critical infrastructure, and personal data on U.S. persons.

[5] CFIUS's new role in real estate transactions

(https://www.dlapiper.com/en/us/insights/publications/2020/02/cfiuss-new-role-in-real-estate-transactions/).