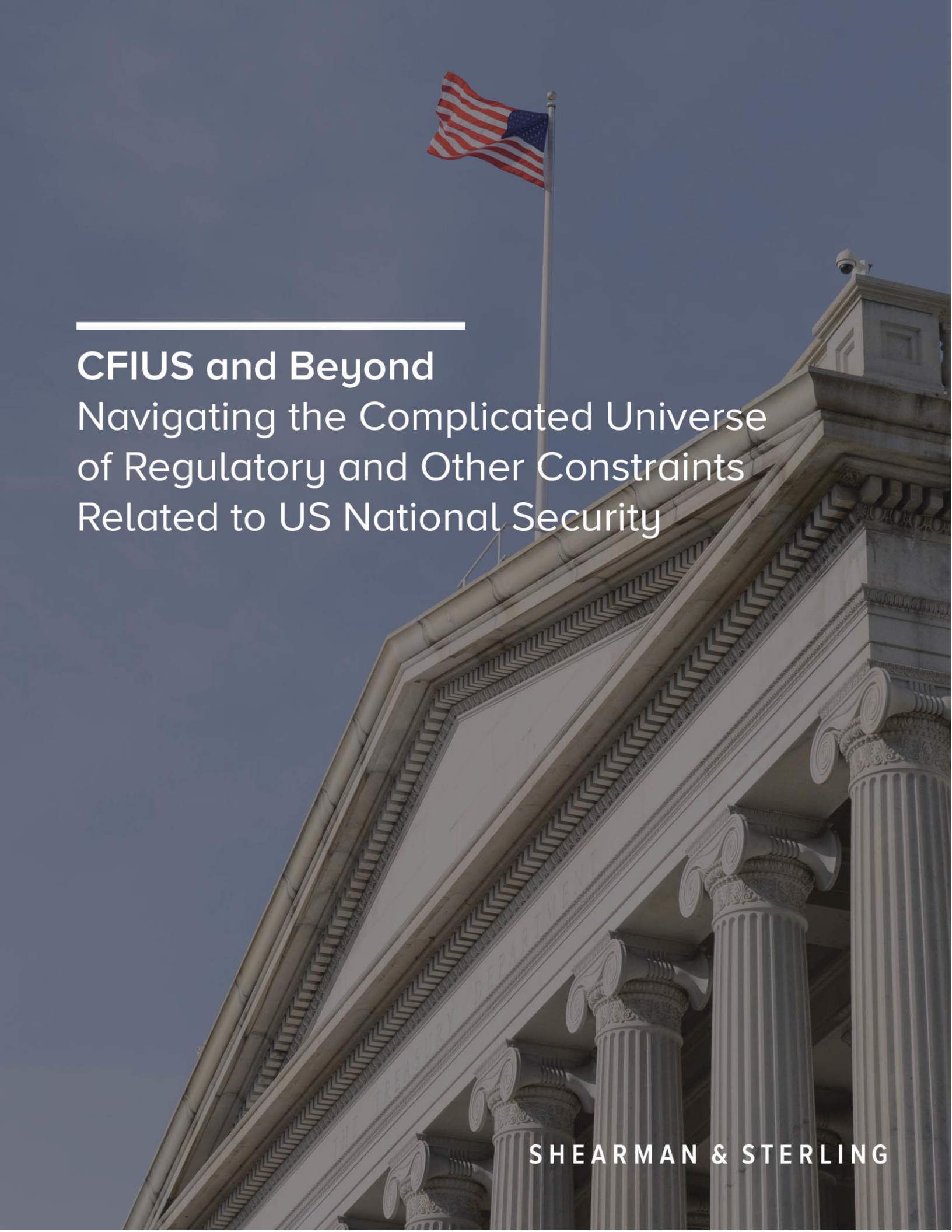

CFIUS and Beyond

Navigating the Complicated Universe of Regulatory and Other Constraints Related to US National Security

SHEARMAN & STERLING

September 8, 2020

The reach and authority of the U.S. government over what it considers to be national security concerns is broad, increasing and often not subject to judicial appeal. In response to mounting threats to the personal, economic and national security of Americans—genuine or not—the U.S. government has implemented, expanded or co-opted extensive regulatory frameworks to protect U.S. national security. This includes reviews of transactions and investments by the Committee on Foreign Investment in the United States (CFIUS) and the newly formed Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (*Team Telecom*), the application of export and supply chain controls by the U.S. Departments of Commerce and State and oversight of the National Industrial Security Program by the U.S. Department of Defense, as well as myriad other licensing and authorizations related to energy, transportation and financial services businesses.

Although these various regimes have evolved separately in response to different potential national security threats, both Congress and the U.S. executive branch have recognized their interplay and their potential as policy tools. In just the past two years, Congress has overhauled the CFIUS process and solidified the committee's connection to U.S. export control laws in an effort to further limit foreign access to U.S. cutting-edge technologies, while the executive branch patched perceived national security gaps in the telecommunications industry by reforming the U.S. government's review of foreign participation in the sector and empowering the Commerce Department to prohibit commercial transactions with foreign infrastructure suppliers further down the supply chain.

In this increasingly challenging regulatory environment, foreign investments in U.S. companies in a wide range of sectors are likely to encounter one or more of these regulatory regimes in a single transaction. It is therefore critical for transaction parties to understand the potential hurdles that may lie ahead before investing their time, capital and reputation so that they can better navigate the regulatory quagmire. While these legal processes can work in parallel, they often have different deadlines and are implemented under different laws, complicating timing and closing decisions. Some require notice of a foreign investment months in advance and others can result in severe limitations on the governance rights of foreign investors or on their access to U.S.-origin technology. Any business that enters this regulatory universe without doing proper diligence does so at its peril.

This article is designed to take at least some of the mystery out of this multi-jurisdictional process by explaining the overlap among these various regimes and the possible impact on proposed foreign investments in the United States.

CFIUS

CFIUS, an interagency committee that conducts national security reviews of certain foreign investments in U.S. businesses, sits at the center of this national security universe. It includes the Departments of Defense, Homeland Security, Commerce, Justice, State and Energy, as well as the Office of the United States Trade Representative and the White House Office of Science and Technology Policy. The Department of Labor and the Director of National Intelligence have non-voting roles.

CFIUS's power primarily stems from its statutory authority to recommend that the U.S. President block or unwind foreign acquisitions of and investments in U.S. businesses when they pose unresolved threats to U.S. national security, following the Committee's assessment of the threat, vulnerabilities, and consequences to national security posed by a transaction. CFIUS also has the authority to negotiate "mitigation agreements" to resolve identified national security threats presented by a transaction. Elements of such mitigation agreements range from prohibitions on transfers of sensitive technologies to protections for U.S. customer data and restrictions on physical and logical access to sensitive U.S. facilities, networks and systems.

Although presidential orders blocking or unwinding transactions are rare, they have increased under the Obama and Trump administrations. The numbers alone do not tell the entire story, as parties will usually terminate a doomed transaction before CFIUS's formal recommendation to block it gets to the president's desk. Moreover, the president's decision is, by statute, not subject to judicial review or other appeal. Although CFIUS is chaired by the Treasury Department, which would seem to be any administration's champion for foreign investment, the national security agencies often co-lead CFIUS reviews, and opposition to a transaction by a single agency can send the matter to the president.

Originally conceived as a narrow check on defense-related foreign investments, the jurisdiction and scope of CFIUS has evolved significantly during the last two decades in response to ever-broadening U.S. national security concerns, such as the 2001 terror attacks on the World Trade Center, the emergence of China as a technological competitor and the threats associated with state-sponsored cyber espionage. The Foreign Investment Risk Review Modernization Act of 2018 (*FIRRMA*), which is the latest congressional overhaul of CFIUS, was undoubtedly intended to protect the technological edge held by the United States by preventing companies from China and other perceived geopolitical adversaries from gaining access to next-generation technologies.

In response to these concerns, FIRRMA and its implementing regulations set forth new rules for investments in U.S. businesses that own or operate critical infrastructure, deal in critical technologies or collect and maintain large amounts of personal data of U.S. citizens (referred to collectively in the regulations as a "*TID U.S. Business*"). The jurisdictional reach of CFIUS, which prior to FIRRMA had been based on whether a transaction could result in "control" of a U.S. business by foreign persons, was expanded further to capture non-controlling investments in TID U.S. Businesses when they grant foreign investors access to material non-public information, board or observer seats, or

significant governance rights. In addition, the new CFIUS regulations require compulsory CFIUS filings or declarations when state-owned enterprises make a "substantial interest" investment in a TID U.S. Business, or when foreign persons make controlling or non-controlling investments in TID U.S. Businesses that deal in critical technologies for specific industry sectors. Lastly, FIRRMA, for the first time, extended CFIUS's jurisdiction to review certain foreign purchases of U.S. real estate.

Other National Security Regulatory Regimes and Controls

While CFIUS's jurisdiction to review acquisitions and investments has been analyzed in great detail since enactment of FIRRMA, what are less well known are the other national security jurisdictions in play and how they intersect and overlap. This is because several of the agency members of CFIUS have independent regulatory regimes through which they can review a proposed transaction and/or have an impact.

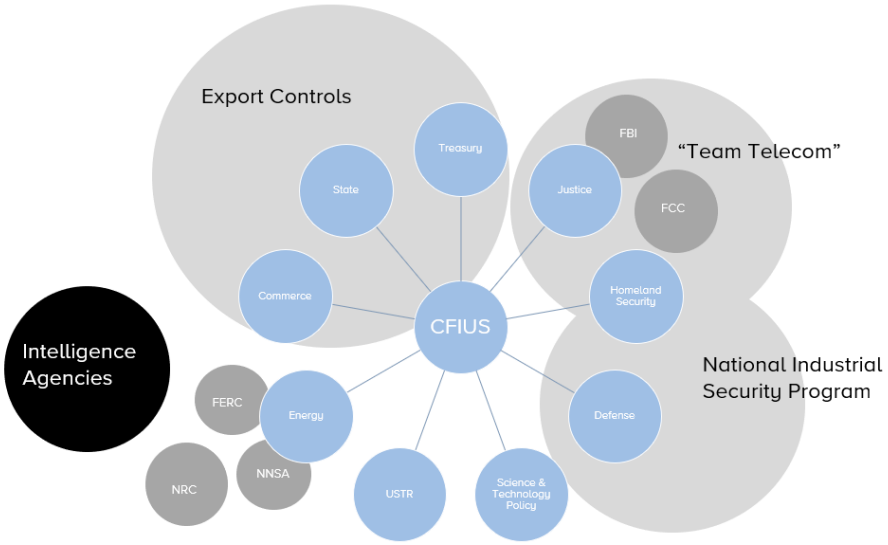

Figure 1: CFIUS and Related National Security Regulatory Environment

Export Controls

Export controls represent one of the most common occurrences of this interplay. U.S. export control laws require that a license be issued by the relevant U.S. government agency before certain U.S.-origin goods or services are exported to certain foreign countries. A failure to comply with these requirements can result in severe fines and even imprisonment. The key export control regimes and requirements include the following:

- **Defense Articles**. Through the International Traffic in Arms Regulations (ITAR), the U.S. Department of State regulates the temporary import and the temporary or permanent export of defense articles and defense services, including hardware that is specifically designed, developed, configured, adapted or modified for a military application, as well as technical data and defense services. Defense articles and services—in the form of hardware, technical data and/or defense services—that are covered by ITAR are listed in the U.S. Munitions List. The export of these items is prohibited without a license issued by the Directorate of Defense Trade Controls, Bureau of Political-Military Affairs at the U.S. State Department.
- **Dual-Use Items**. The U.S. Commerce Department regulates what are called "dual-use" items—*i.e.*, U.S.-origin civilian products, materials, technology, technical data and software that have potential military applications—through the Export Administration Regulations (EAR). EAR export controls generally do not prohibit the sale of U.S.-origin goods or technologies to a given destination country, although there are several lists of persons and entities to whom such exports are prohibited. Instead, the export (or re-export) of certain categories of U.S.-origin goods, technologies or technical data to certain countries requires an export license issued by the Bureau of Industry Security at the Commerce Department. Recent amendments and proposed amendments to the EAR have greatly expanded the reach of export controls to certain destination countries.
- **Sanctions**. The U.S. Department of Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, individuals and regimes. Unless licensed by Treasury's Office of Foreign Assets Control (OFAC), goods, technologies or services generally may not be exported, re-exported, sold or supplied, either directly or indirectly, from the United States or by a U.S. person, wherever located, to any sanctioned country, person or entity. Economic sanctions

administered by OFAC are classified as either "country-based" or "list-based" programs. Country-based economic sanctions programs prohibit almost all transactions between U.S. persons and the targeted country. The prohibition extends to transactions between U.S. persons and the targeted country's representatives or state-owned companies, and, in some cases, citizens no matter where located. List-based economic sanctions programs prohibit transactions between U.S. persons and specific individuals and entities allegedly engaged in disfavored activities, including narcotics trafficking, international terrorism and proliferation of weapons of mass destruction. The targets of these programs are designated as "Blocked Persons" and are listed on the "Specially Designated Nationals and Blocked Persons List." Because OFAC frequently revises these programs, it is important for transaction parties to regularly check for updates.

- **Re-Exports**. U.S. export controls apply to so-called "re-exports." A "re-export" occurs when U.S. goods or technologies originally are shipped from the United States to one country and then exported from that country to another third party country. For example, a re-export would occur when a good that was originally shipped from the United States to a European country is incorporated into a European product that is subsequently sold to another country. The production of certain commodities outside the United States using certain US technologies is also considered a re-export. Where U.S. goods or technologies have been substantially transformed outside the United States into a foreign-made product, the re-export of this product, however, may be excepted from U.S. export controls. Recent regulations impose additional restrictions on exports to certain countries of certain items.
- **Deemed Exports**. U.S. export control laws also restrict "deemed exports," or the transfer of technology or technical data within the United States to a person who is a non-U.S. national. As a result, any non-U.S. nationals employed by a foreign company at its facilities in the United States may face additional restrictions on their ability to handle, view or work with U.S.-origin technology or technical data. These are complex issues, however, requiring fact-intensive analysis, and this overview does not capture the nuance in this area of the law.

There are many components to compliance with these requirements. If U.S.-origin goods, technologies or technical data are subject to any U.S. export controls, the exporter (which could include the producer, the developer or the actual exporter) must determine

whether an export license is required to export to a given country or end-user. The license application process involves providing the applicable agency with information relating to the product, technology or technical data desired to be exported, as well as the end-user and any intermediaries. To ensure ongoing compliance with U.S. export controls and other applicable laws, all exporters should implement an effective export controls compliance program. This is critical to preventing and detecting violations of applicable laws and, in the event that a violation does occur, an effective compliance program can help to mitigate the penalties imposed by the U.S. government.

Moreover, investments in or acquisitions of U.S. businesses that deal in items covered by export controls will face heightened scrutiny by CFIUS as well as separate reviews in many cases. There is no guarantee that an export license for a given product, technology or end-user will be granted. The grounds for control and the identity of the destination country and the end user will have a significant effect on the likelihood that an export license will be granted.

> **How the National Security Regimes Interact: Export controls are relevant to transactions involving foreign investors in a number of ways. First, FIRRMA clearly links the responsibilities of CFIUS with those CFIUS member agencies that administer U.S. export control laws, especially the Commerce Department. FIRRMA includes the "Sense of the Congress" that "the national security landscape has shifted in recent years, and so has the nature of the investments that pose the greatest potential risk to national security, which warrants an appropriate modernization of the processes and authorities of [CFIUS] and of the United States export control system." Second, the definition of "critical technologies," which is central to FIRRMA, has primarily been based on whether products are subject to U.S. export controls. FIRRMA added to the law's definition of critical technologies "emerging and foundational technologies controlled under section 1758 of the Export Control Reform Act of 2018, which was companion legislation enacted alongside FIRRMA. Those emerging and foundational technologies are currently being identified through an ongoing process conducted by the three primary export control agencies—the Departments of Commerce, State and Energy. Finally, all of those agencies are statutory members of CFIUS and regularly lead CFIUS reviews relevant to their particular expertise.**

From conducting due diligence to negotiating transaction provisions to closing a transaction, both foreign "buyers" and U.S. "sellers" need to take this inter-relationship into account. For example:

For Buyers:

- Export compliance has long been a focus of CFIUS national security reviews. Buyers, whether foreign or U.S., need to be aware that they will be inheriting any liability from the unmitigated export control violations of the target company. In addition, transactions before CFIUS can be held up if significant export control violations are discovered during the CFIUS review. For that reason, buyers should generally request information on whether the seller manufactures products, provides services or has developed technology subject to U.S. export controls, and ask how the seller arrived at its conclusions regarding export classification. Buyers should generally ask to review the seller's export compliance program, which should be tailored to the seller's business and implemented throughout the seller's organization. In addition, buyers should ask whether the seller has been found to have violated U.S. export controls or submitted voluntary self-disclosures to the relevant agencies. Buyers should also consider asking for a warranty or representation related to export controls.
- As part of this due diligence process, buyers should also generally ask whether the seller's products, technology or services have military applications or are covered by ITAR, and whether the seller is an ITAR registrant. In addition to potential licensing issues under ITAR, there will be mandatory notice requirements to the State Department if the U.S. business is being sold to a foreign person or if the investment represents a material change to the information originally supplied to the State Department.
- Although it may seem obvious, foreign buyers should gauge whether licenses for technology that is essential to running a target U.S. business are likely to be approved given the buyer's nationality. That analysis, as well as a decision on whether to invest in a U.S. business, should take into account the policy and political environment at the time.
- Buyers also need to be aware that they will almost certainly be asked during the CFIUS review process whether they have done business with countries subject to U.S. and UN sanctions.

For Sellers:

- As noted, the export control agencies have their own regimes that license exports and have the authority to assess enormous fines, and in certain cases imprison those who violate U.S. export control laws. Sellers who have products,

technology or services subject to U.S. export controls should confirm, before undergoing CFIUS review, that they have no export control violations and consider filing a voluntary self-disclosure if they do. They should also ensure that they have a tailored export compliance plan in place.

- During due diligence, sellers must be very careful about what materials and information they make available in a data room, as foreign persons from a country for which U.S. export control laws require a license may not have access to covered technology located without a license.

Both buyers and sellers should be aware that any revelation during the CFIUS process of export control violations could have an impact on the outcome of a CFIUS review or at least the timing of obtaining CFIUS clearance. As the Departments of State, Energy and Commerce all are CFIUS member agencies, they will likely request that CFIUS not clear the transaction until any alleged violations are cleared up. This could have an impact on the timing of the close of the transaction. The above represents just some of the issues related to export controls that can arise in transactions involving foreign investments in U.S. businesses. Mergers, acquisitions and investments are, of course, fact specific and require measures that are tailored to particular transactions. This article provides an overview of these and other complicated issues but should not in any way be interpreted as legal advice.

The Telecommunications Sector: Team Telecom and Commerce Department National Security Authority

In April 2020, the President issued an executive order formalizing and expanding the *ad hoc* review process that has governed investments in the U.S. telecommunications services sector for more than 20 years. This order specifically created a formal "Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector" (colloquially referred to as "Team Telecom") and charged it with assisting the Federal Communications Commission (FCC) in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the U.S. telecommunications services sector. The order designates the Departments of Defense, Homeland Security and Justice as formal members and names the Department of Justice as the chair. Certain other agencies and branches of the U.S. government are designated as informal advisors to the Committee, including the Departments of State, Treasury and Commerce and the Director of National Intelligence.

The executive order provides Team Telecom with broad authority in two key areas. First, Team Telecom can review the national security and law enforcement implications arising from applications submitted to the FCC that seek new telecommunications or spectrum licenses by foreign-owned or controlled entities, or FCC approval for transactions involving foreign ownership of FCC-licensed carriers. Team Telecom can also undertake a review of any existing FCC license holder to determine whether maintaining, granting or transferring a license would pose a risk to the national security or law enforcement interests of the United States.

Importantly, the executive order formalizes and creates firm processes and deadlines by which Team Telecom must act and complete its analysis. Once Team Telecom receives an application referral from the FCC, it must undertake an initial review of the application. As part of this initial review, Team Telecom assesses whether granting the application will pose a risk to national security or U.S. law enforcement interests. At the end of the initial review, Team Telecom may determine and notify the FCC that the application does not raise any national security or law enforcement concerns, or that "standard mitigation measures" would resolve such concerns. Team Telecom must complete this initial review within 120 days of determining that the applicants had responded completely to any questions or information requests. Team Telecom may undertake a secondary assessment after determining that any risks identified during its initial review cannot be mitigated through standard measures. This secondary review must be completed within 90 days after the Committee determines that a secondary review is warranted.

With respect to applications seeking FCC approval for corporate transfers of control or new licenses, Team Telecom can make one of three recommendations to the FCC: (i) that it has no objection to the FCC granting the license or transfer of the license; (ii) that the FCC should deny the application due to risks to the national security or law

enforcement interests of the United States; or (iii) that the FCC should only grant the license or transfer of the license contingent on the applicant's compliance with mitigation measures determined by Team Telecom. With respect to its authority to review existing licenses, Team Telecom can make one of three recommendations to the FCC: (i) modify the license to include a condition of compliance with negotiated mitigation measures; (ii) revoke the license due to risks to national security or law enforcement interests of the United States; or (iii) take no action with respect to the license.

As noted above, Team Telecom is focused on ensuring that FCC-licensed operators present no concerns for U.S. national security or law enforcement interests. However, other recent presidential actions have expanded the U.S. government's efforts to protect the U.S. telecommunications grid to also include participants in the supply chain. In May 2020, the President signed an executive order extending national security oversight to transactions implicating the telecommunications supply chain, including through imports and contracts for telecommunication technology, inputs and services. Relying on his authority under the International Emergency Economic Powers Act, the President's order authorizes the Commerce Department, working in conjunction with most of the CFIUS agencies, the FCC and the Director of National Intelligence, to prohibit a range of telecommunications transactions involving technology, products or services that are "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." The order defines "foreign adversary" as "any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."

The interagency group may take such action when it determines that telecommunications transactions involving persons and property subject to U.S. jurisdiction pose "an undue risk of sabotage to U.S. information and communications technology or services; an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or otherwise poses an unacceptable risk to the national security of the United States." As with CFIUS and Team Telecom, the Commerce Department may negotiate measures to mitigate such concerns and take action to prohibit the offending transactions.

> **How the National Security Regimes Interact: It is clear the U.S. Government considers telecommunications networks and infrastructure to be among the country's most strategic assets. The member agencies of Team Telecom are also members of CFIUS, so there is a considerable overlap between the two review processes. Both regimes have the authority to condition approval of transactions on agreement by the parties to accept mitigation measures. Both regimes also can, to some extent, take a second look at an approved transaction or existing license.**

Impact on Parties to Telecommunications Transactions:

- Buyers and sellers engaging in telecommunication transactions need to be aware of the scope and limits of these overlapping review processes. At the outset, transaction parties must view Team Telecom as effectively a mandatory national security review process, given that the FCC will not grant an application or request that has been referred to Team Telecom until it has received Team Telecom's clearance. This is different than CFIUS in which compulsory reviews apply only in very narrow circumstances.
- Transaction parties must also understand that the Team Telecom review process is not implicated in every telecommunications transaction. Indeed, the FCC only will refer applications or transactions to Team Telecom if they result ultimately in the foreign ownership or control of an entity holding a common carrier or spectrum license. This stands in contrast to CFIUS, which has the authority to review acquisitions of, or investments in, U.S. telecommunications entities regardless of the specific FCC licenses they may hold.
- Lastly, parties need to keep in mind that, despite the new Team Telecom deadlines, the timelines for Team Telecom and CFIUS reviews do not track in all respects. It is thus important to factor the timing of each separate review into anticipated closing timelines of any transaction.

The National Industrial Security Program

The U.S. National Industrial Security Program (NISP), largely administered by the Defense Counterintelligence and Security Agency (DCSA) at the U.S. Department of Defense (DOD), prescribes requirements, restrictions and other safeguards to prevent unauthorized disclosure of classified U.S. information, which include clearances, special security agreements and secured facilities. Any foreign acquisition of a U.S. entity that performs on classified contracts or has access to classified U.S. information will likely be subject to a CFIUS review, as well as a separate review by DCSA to assess the impact of the "foreign ownership, control or influence" (FOCI) on the U.S. entity. The goal of the FOCI review is to ensure foreign buyers do not undermine U.S. security or export controls to gain access to U.S. critical technology or classified information.

In making this determination, DCSA will consider, among other things, the source, nature and extent of FOCI, including whether foreign interests hold a majority or substantial minority position in the company, taking into consideration the immediate, intermediate and ultimate parent companies. A minority position is deemed substantial if it consists of greater than five percent of the ownership interests or greater than ten percent of the voting interest. If FOCI is found to be present, DCSA will require some kind of agreement or arrangement to mitigate foreign influence and potential access by foreign persons to classified information. Similar to CFIUS, such mitigation can range from putting in place security measures to ensure there will be no foreign access to classified information to, under a proxy agreement, requiring a fully independent board to oversee the U.S. entity, depending on the amount of FOCI.

> **How the National Security Regimes Interact: As with transactions falling within the jurisdiction of CFIUS and the Committee, parties to deals involving access to classified information must manage two parallel processes, one with CFIUS and one with the Defense Department or other contracting agency. In fact, NISP provides that if the contracting agency "becomes aware of a proposed transaction that should be reviewed by CFIUS, and the parties thereto do not file a joint voluntary notice with CFIUS to initiate review within a reasonable time, the [contracting agency] shall initiate action to have CFIUS notified."**

Timing is also an issue here, and foreign buyers in some cases will have to assess whether they are willing to accept a proxy in which they will have very diminished governance rights over a company they own. It is generally advisable to commence the FOCI process before formally filing with CFIUS. U.S. businesses handling classified contracts must be careful not to expose classified information to foreign persons during the negotiating, due diligence or transition processes.

Energy

The U.S. Department of Energy (DOE) is an active participant in the CFIUS review process and separately conducts its own licensing reviews in its capacity regulating the interstate transmission of electricity, natural gas and oil through the Federal Energy Regulatory Commission (FERC). Through the National Nuclear Security Administration (NNSA), it also manages all activities relating to the U.S. nuclear weapons stockpile, coordinates certain domestic and international nonproliferation activities and provides nuclear propulsion plants for the United States Navy. The U.S. Nuclear Regulatory Commission (NRC) is an independent agency that regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements. DOE and NRC also serve as Cognizant Security Agencies under the NISP and administer certain industrial security programs to protect specific energy-related materials, assets and data.

> **How the National Security Regimes Interact: Any transactions involving any FERC, NNSA or NRC licenses, authorizations, facilities and/or activities can expect heightened scrutiny and separate restrictions on foreign investment.**

Intelligence Agencies

The Director of National Intelligence is an independent agency, a non-voting member of CFIUS and also a Cognizant Security Agency under NISP charged with protecting intelligence sources and methods, including classified information and data. In addition, there is the Central Intelligence Agency—also an independent agency—and numerous other intelligence organizations throughout the executive branch, including the U.S. Departments of Defense, Homeland Security, Energy, Justice, State and Treasury.

These intelligence organizations provide input and information to CFIUS and other agencies during the course of their reviews. In addition, there are some U.S. businesses that have contracts with some of these organizations or are subject to certain restrictions or manufacturing specifications. Most foreign investment in any such U.S. businesses will not be highly scrutinized.

Timing

All of these different processes are generally undertaken concurrently. Foreign acquisitions or investments in U.S. businesses that involve the telecommunications sector, for example, will be subject to a CFIUS review, as well as reviews by the Committee and the FCC. If that U.S. business also involves technology that is controlled for export, it will be subject to review by the U.S. Departments of State and or Commerce. If that U.S. business also has classified information, it will be subject to a review by the U.S. Defense Department. Thus, the reach of the U.S. government is much broader than what is initially obvious and greatly expanded from what it used to be. The common theme is national security and what measures are necessary to protect each sector from dangerous foreign access.

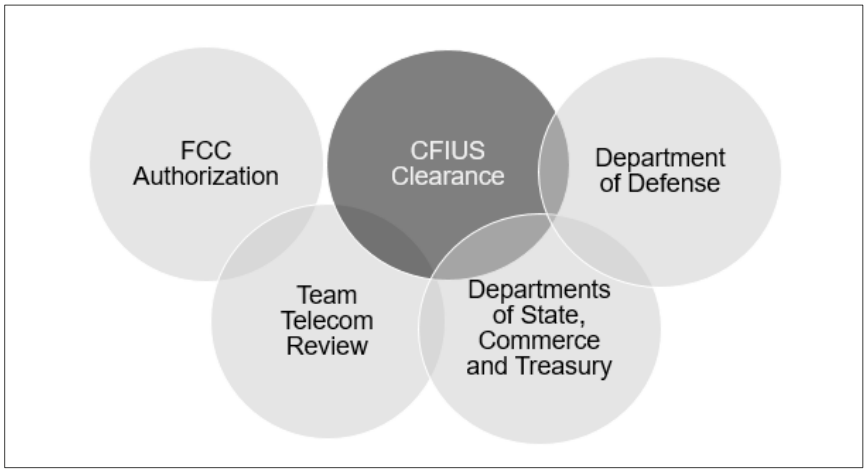

Figure 2: Potential Overlap of Multiple Regulatory Regimes

All of these reviews will be on different timelines, some with no deadlines, and will focus on similar issues but will have different requirements. And, usually, all will need to be completed before the transaction can close.

Thus, we also recommend that clients factor CFIUS and other regulatory review timing into the deal schedule.

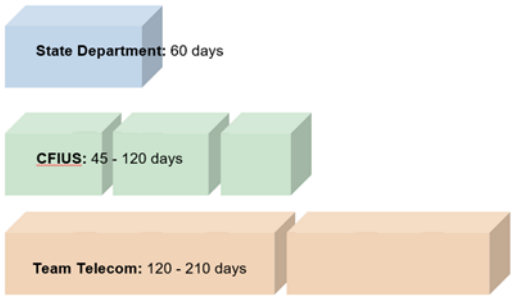

Figure 3: Sample Minimum Timeframes

Conclusion

In closing, it is important to consider both the practical implications and regulatory landscape in planning a transaction. Failure to consider CFIUS and other national security-related issues can have a severe impact on a proposed investment or acquisition. It can slow it down or, post-closing, lead to the unraveling of the transaction. It can also lead to post-closing mitigation demands by the U.S. government. It can result in a failure to close in the agreed-upon time frame and expose buyers and sellers to risk of break-up fees and additional legal fees. It can expose the parties to scrutiny for export control and other violations of U.S. law. It can lead to post-closing scrutiny by CFIUS and other U.S. government agencies.

Thus, we recommend clients flag potential national security concerns as part of the due diligence process, focusing on the following:

- **Security** – sensitive U.S. assets, access to classified information, U.S. government contracts
- **Sector** – defense, energy, telecom, data management and information security
- **Location** – proximity to sensitive U.S. assets
- **Export Controls** – military, dual use or missile technology
- **Acquirer** – nationality of concern; whether or not state-owned

The trend of heightened scrutiny of foreign investment is here to stay and must be treated as a key consideration in all transactions involving foreign buyers. The keen focus on national security factors did not begin with the Trump Administration and is unlikely to significantly change for the foreseeable future.

Authors & Contributors

John M. Beahn

Robert S. LaRussa

Lisa S. Raisner

Related Services

Practice
CFIUS

Region
North America