Remarks by Assistant Secretary for Investment Security Paul Rosen at the Second Annual CFIUS Conference

September 14, 2023

As Prepared for Delivery

Thank you, Leila, for that introduction. And thank you for serving in this newly created role as the first Chief Counselor for Enforcement on CFIUS matters at Treasury.

Good afternoon, everyone. A big thank you to our panelists today for a frank and insightful discussion. Each of you is a close partner, and I appreciate the outstanding effort you put into our mission. I also see many members of the CFIUS bar in the audience. I want to thank you all for your hard work, which we know can be challenging under the very best of circumstances. And, last but not least, thank you to Meena Sharma, our head of Policy & International Relations, for her and her team’s work in creating and shaping what is now an annual gathering of our broader CFIUS community.

It is a pleasure to update you on the Committee’s compliance and enforcement priorities and highlight how we are going about this work. This includes the various tools available for the Committee to address potential national security risks, and a forecast of some of what we expect in the coming months and year. I will touch on transaction reviews, mitigation agreement monitoring, third-party processes, non-notified transactions, penalties, and some anticipated regulatory updates.

CASE PROCESSING AND TRANSACTION REVIEWS

Starting with the transaction review side, we continue to sharpen our diligence. We carefully examine transaction structures and ownership, and—where necessary and appropriate—probe investment agreements or arrangements, including with limited partners.

In that regard, over the last year we have had a number of situations I would like to raise as examples of ways we ensure the Committee is addressing national security risk:

- We’ve required the submission of confidential side letters entered into with investors, including with limited partners, where it was relevant to our national security
We’ve imposed mitigation agreements on an interim or permanent basis in certain circumstances, such as when parties have refused to negotiate or agree to necessary terms to protect national security—and we are now enforcing those agreements; and

- We are prepared to file an Agency Notice when parties refuse to file or cooperate with the Committee—putting a case and parties on the clock and under review involuntarily.

At the same time that we are taking these steps, we recognize the vast majority of parties work with and cooperate with CFIUS. We know the CFIUS process can be complicated. It can be resource intensive. And—in some instances—it can affect timelines and introduce other dynamics to market transactions.

As a result, we work to balance and moderate these effects, and we will continue to carefully use our tools when appropriate to carry out our national security mission.

**MONITORING OF MITIGATION AGREEMENTS**

One example of this is with respect to cleared cases and mitigation agreements: When a case is cleared where a risk is identified, it is typically because parties have signed up to a mitigation agreement with the U.S. government. Our statistics from 2022 show that about 23 percent of our notices concluded with mitigation agreements, amounting to 41 transactions last year, up from 26 the year before. However, this was not always the case.

CFIUS negotiated its first mitigation agreement in 1997. Ten years later, in 2007, Congress passed the Foreign Investment and National Security Act, or FINSA, which codified the procedures and processes with respect to risk mitigation agreements, monitoring, and enforcement that we know today.

Specifically, FINSA authorized the Committee to enter into, modify, and monitor mitigation agreements and directed us to enforce compliance with these agreements. In 2018, the Foreign Investment Risk Review Modernization Act, or FIRRMA, strengthened the use of mitigation agreements, including the addition of compliance plans, and codified the process to identify non-notified transactions. We now have more than 230 active mitigation agreements. These agreements vary—some are relatively straightforward with only a few terms, others are complex agreements that address a range of business activities and set forth various obligations and reporting requirements on the parties. In each case, every term is directly related to a risk we have identified and is important for protecting national security.
As we carry out this work, we are renewing our focus on compliance and ensuring we have the necessary resources to do so. This means parties can expect more compliance checks, questions, and site-visits. We are also leaning on third-party monitors and auditors and are actively engaged with them. We are particularly focused on parties having a plan for how they will comply with mitigation agreement terms, as we’ve seen in our enforcement work what can happen when that was not the case.

With regard to site visits for companies with active mitigation agreements, some may have noticed increased volume, attention, and follow up in the last six months. Parties can expect more of that. Parties can also expect the site visit team to conduct interviews at all levels, including of line-level staff, perform spot checks on records, and engage in other measures to actively monitor compliance of mitigation agreements.

**IMPROVEMENTS TO THIRD-PARTY PROCESSES**

As our mitigation work increases, we are bolstering the already significant resources we dedicate to monitor compliance. We also rely on third party auditors or monitors in some agreements. We recognize the burden that such oversight can impose on parties, which is why we make every effort to deploy this tool only when necessary to protect national security.

For example, third-party monitors and auditors provide oversight of compliance of matters that require particular technical expertise like quantum computing or biotechnology. Mitigation agreements also often require access controls and procedures for protecting sensitive data and technology. Third-party monitors do not just monitor and report on compliance; they also often advise the security officer, director, and other compliance staff within companies on key process improvements. In these instances, their work is critical in not only facilitating compliance but also in devising improvements and other measures to eliminate national security risks.

With this in mind, the Committee has taken steps over the past year to sharpen the use of third-party providers. We have been working to expand the number of monitor and auditor firms engaged in this work, including those who have not traditionally been active in the CFIUS space. Treasury has held meetings with vendors to discuss procedures for nominating individuals as well as standards and expectations. Indeed, we know that the cost for such services can be significant, and we expect active involvement and rigorous analysis when it comes to the execution of their responsibilities.
In addition, we have worked to improve our vetting, selection, and monitoring processes for third-party providers to ensure they can fulfill the increasing responsibilities they carry. This includes analysis of qualifications and work plans and adjustments to how CFIUS will approve third-party providers going forward. We won’t hesitate to replace third party providers if they are not meeting expectations.

NON-NOTIFIED TRANSACTIONS

Our non-notified work is one of CFIUS’s most important functions, and we remain focused on the transactions of concern that may be subject to CFIUS jurisdiction but are not filed. Filing with CFIUS is largely voluntary. And we don’t know what we don’t know. Yet through our non-notified work, we seek to know—and act upon what we find—when in the interest of national security.

Accordingly, we are adding resources to detect and bring in non-notified transactions. In 2022, we requested filings for 19 non-notified transactions. These transactions were carefully vetted and many ended up in mitigation or voluntary divestment. Our focus in this area continues. We have added resources to reinvigorate the attention we give to failures to file. We also finalized several inquiries into such matters and have more in the pipeline, including deals valued at hundreds of millions of dollars. Parties should remember that the failure to file a mandatory declaration can lead to penalties of $250,000 or the value of the transaction, whichever is greater.

PENALTIES

The activities that I’ve described thus far are meant to maximize compliance in the interest of national security. And the vast majority of parties take their obligations seriously. But violations of mitigation agreements and CFIUS regulations do occur, and we have taken enforcement action and issued penalties to address violations when they happen.

Under CFIUS’s statute—the Defense Production Act—the Committee has enforcement authority, including subpoena authority. We can impose monetary penalties and seek other remedies for violations of our statute and regulations. Violations can occur when companies fail to file mandatory declarations or comply with mitigation agreements, orders, or other conditions.

Last year, the Committee also issued its first-ever CFIUS enforcement and penalty guidelines. While the guidelines reflect long-standing principles of the Committee, they were codified in
writing for the first time to provide the public and practitioners with additional transparency about how we assess and penalize violations.

In evaluating whether to bring enforcement action and the appropriate type to pursue, there is a robust process by which the Committee reviews the specific facts and circumstances surrounding the violation. These facts include the party’s compliance history, any aggravating and mitigating factors such as self-disclosure of the violation, cooperation with the Committee’s investigation, the frequency and duration of the conduct, and the extent to which the conduct impaired or threatened to impair U.S. national security. The Committee takes seriously our obligation to look closely at the various aggravating and mitigating factors and the facts and circumstances of each matter when determining the proper action.

A key part of the guidelines is its emphasis on the importance and benefits of voluntary self-disclosure of violations, which can be a significant mitigating factor that informs the determination of whether and what type of enforcement action to pursue. Self-disclosure to the Committee of violations is an important step in protecting national security, as it helps identify and address violations. As a result of this guidance, the Committee is receiving more voluntary self-disclosures, including for violations of mandatory filing requirements.

When violations occur, whether they be intentional or inadvertent, the message I have delivered as Assistant Secretary is that the Committee will respond to protect national security. Enforcement actions—through civil monetary penalties, remediation plans, or warning letters—hold parties accountable. They also serve to deter future breaches and remediate immediate or long-term risks to national security.

Here at the Treasury Department, we have been doubling down on efforts to improve our protocols and train our staff to focus on enforcement best practices. As mentioned, we hired our first ever Chief Counselor for Enforcement to help us work cross-functionally across the Department and coordinate our team’s handling of cases from day one. Prior to this year, the Committee has issued only two civil monetary penalties. So far in 2023, we have issued two civil monetary penalties, and have several more pending at various stages. We are on track to have more civil monetary penalties issued this year than we have in our entire history. This is on top of various warning letters and other actions that we have taken in response to violations of CFIUS regulations. This work reflects our twin focus on ensuring accountability as well as ensuring that we take a deliberate, careful, and analytical approach to our penalty assessments, which can take time. We intend to share more with the public when appropriate to promote transparency and advance our national security objectives.
These changes should incentivize companies considering *investment* in the U.S. economy by providing further transparency, and should also importantly provide support for outside counsel, general counsel, compliance officers, and boardrooms to also *invest* in CFIUS compliance, monitoring, and prompt disclosure.

**ANTICIPATED REGULATORY UPDATES**

Finally, I want to say a word about some anticipated upcoming regulatory updates. As you all know, FIRRMA modernized CFIUS and the legislation led to the issuance of detailed implementing regulations. It’s time to refine some of those regulations, so over the course of the next year I expect that Treasury will be issuing one or more notices of proposed rulemaking to do so. I expect these updates to include measures that (1) allow for increased efficiency and effectiveness in our case processing and review functions, (2) update the Committee’s penalty and enforcement authorities, (3) sharpen and enhance the Committee’s tools in the non-notified space, and (4) broadly ensure the Committee’s tools and processes are best aligned to the current landscape. Stay tuned for the details of this rulemaking and please provide your comments in the rulemaking process.

**CONCLUSION**

As I finish my remarks today, let me conclude on one important point:

The Committee very much values the working relationship we have with companies and firms who file with the Committee and their counsel. The best results for national security and economic growth are achieved when we are working together. We look forward to continuing to do so. Thank you.

###