

## **CFIUS and the “America First” Investment Policy: Nine Recommendations for Executive Action**

October 6, 2025

Stephen Heifetz  
Wilson Sonsini Goodrich & Rosati

Andrew Grotto  
Stanford University

### **I. Introduction**

In early 2025, President Donald Trump unveiled his “America First Investment Policy,” an effort to make the United States a more appealing destination for foreign capital from U.S. allies. Since then, President Trump has secured commitments from many trading partners to significantly ramp-up their investment in the United States. Regulators now should focus on reducing red tape and eliminating unnecessary barriers to investment to ensure that this wave of foreign capital generates returns for the American people and advances U.S. national security.

One area ripe for reform is the Committee on Foreign Investment in the United States (CFIUS), an interagency regulatory body chaired by the Treasury Department and accountable to the President. CFIUS conducts screening of foreign investments into the United States for national security risks. The CFIUS process is intended to keep sensitive American technology, data, products, real estate, and services away from malign foreign actors, while maintaining an open-investment climate that attracts desirable foreign investment.

*About the authors: Heifetz is a practicing CFIUS attorney. Grotto founded and co-directs the Program on Geopolitics, Technology, and Governance at Stanford University and previously served on the National Security Council in the Obama and Trump I administrations. All views presented here are the authors' alone, as are any errors or omissions. For correspondence: grotto@stanford.edu.*

In 2018, President Trump signed the Foreign Investment Risk Review Modernization Act (FIRRMA), which expanded the range of transactions subject to CFIUS jurisdiction. Seven years later, we now have sufficient experience with the practical operation of the post-FIRRMA CFIUS process to identify friction points that do not meaningfully advance U.S. national security and unnecessarily raise the costs of investing in the United States. We offer nine recommendations that could be implemented by executive action alone, whether by President Trump or his deputies at CFIUS, to resolve these issues.

## **II. Background**

When a foreign investor considers investing in a U.S. business, an important factor is whether the transaction would trigger an expensive, lengthy, and potentially deal-killing review by CFIUS. CFIUS regulations mandate that for certain foreign investments, the transacting parties must seek approval from CFIUS. While a small number of transactions are subject to mandatory CFIUS filings, a much larger number are subject to CFIUS's elective jurisdiction, meaning that CFIUS may conduct a review of the transaction even if the parties are not required to file. Parties pursuing transactions that are not subject to CFIUS mandatory filing requirements still may choose to submit a "voluntary" filing to CFIUS because obtaining CFIUS approval insulates the transaction from adverse CFIUS action in the future (such as forced divestment).

The parties apply for CFIUS approval by disclosing certain details about the transaction in a confidential national security filing. CFIUS uses information from these filings and other sources – such as classified intelligence, publicly-available data (e.g., newspapers, federal trade and economic data, and SEC disclosures), and commercial research platforms (e.g., Bloomberg) – to assess each filed transaction for national security risk. If CFIUS determines the transaction presents national security risk, CFIUS can make a recommendation to the President to block the transaction, or CFIUS can condition its approval on whether the transacting parties accept security-related commitments – so-called "risk mitigation agreements" or "mitigation measures" – to address CFIUS' national security concerns.

Every year, there are more than 10,000 transactions within CFIUS's jurisdiction that CFIUS *could* review and with respect to which the transaction parties (or their counsel) must consider and weigh CFIUS rules and risks – even if CFIUS never elects to conduct a review. For the past several years, CFIUS has reviewed 300-500 transactions annually, primarily in response to voluntary and mandatory filings by transaction parties (CFIUS also may review transactions that were not filed). CFIUS annually intervenes in a few dozen of these

transactions either by recommending that the President block the transaction or by conditioning CFIUS approval on the parties agreeing to mitigation measures, such as limiting foreign access to data or granting CFIUS veto rights over significant corporate decisions (as [recently manifested in the Nippon-U.S. Steel matter](#)).

The CFIUS process aims to bolster national security, but it also generates significant costs for U.S. businesses and investors. These costs include deals that are deterred, delayed, or reduced in scope (e.g., it has become common for investors to cap their minority investments at less than 10% equity because 10% is a relevant threshold for CFIUS jurisdiction); lawyer fees; compliance with mitigation conditions imposed by CFIUS; and the outlays of taxpayer dollars to finance CFIUS's operations.

In the aggregate, these constitute substantial costs for the U.S. economy. Particularly for the start-up technology ecosystem, a key driver of U.S. innovation, the CFIUS review process can eat a significant portion of raised capital that otherwise could be invested in start-ups. CFIUS therefore makes access to capital harder for these start-ups, including those whose businesses could directly support U.S. national security. This is so even with respect to investments from closely allied countries. A start-up robotics company might eventually contribute to U.S. military power, for example, but the higher cost of capital that the CFIUS process requires (e.g., because a foreign investor may elect to stay below the 10% equity threshold and/or because of other costs associated with complying with the CFIUS review process) makes it less likely that the start-up will ultimately grow into a mature company that can actively contribute to U.S. defense.

While some costs are inherent to the CFIUS process, our review of that process – as it is experienced by transacting parties and their lawyers – has identified numerous friction points that are ripe for reform because they do not meaningfully contribute to national security, they impose unnecessary costs on transacting parties, and they distract CFIUS from more pressing matters. This white paper, drawing on consultations with dozens of lawyers – who collectively have provided counsel on tens of thousands of transactions over decades of practice – describes these key friction points and potential resolutions. We identify nine efficiency recommendations that, if implemented, would streamline the CFIUS process, reduce transaction costs for investments into U.S. companies, and ultimately make America a more attractive destination for foreign investment – with no material adverse impacts on national security.

### III. Summary of Recommendations

The following nine recommendations, discussed in-depth later in this paper, would require *no changes to the legislation or regulations that govern CFIUS*:

- Publish anonymized “covered transaction analyses.”
- Rescind the “completion date” FAQ.
- Designate an “Efficiency Advocate” within the Treasury Department.
- Mandate that CFIUS may not propose mitigation measures unless the Deputy Secretary from the lead CFIUS agencies agree such measures are both necessary and narrowly tailored to resolve national security risks.
- Establish standards for third-party monitors and auditors.

The following recommendations would require amending CFIUS regulations but would not require legislative action by Congress:

- Simplify the scope of “critical technology” that can trigger a mandatory CFIUS filing; at a minimum, remove encryption items from this scope (there is vociferous practitioner consensus on removal of encryption from the scope of mandatory filing triggers).
- Exempt benign corporate reorganizations from the scope of mandatory filings.
- Reduce the stringency of “excepted investor” qualification standards.
- Implement the “Known Investor” program announced by Treasury earlier this year.

Congress also could consider legislative changes to improve CFIUS efficiency. We focus here, however, on changes the administration could implement swiftly with executive action.

### IV. Three Layers of Costs

CFIUS imposes costs – money, time, and opportunity costs – at three different layers.

- Layer One -- Assessment: Parties to **thousands of transactions** each year consider relevant CFIUS risks and requirements. Transaction parties may expend considerable time and resources to assess CFIUS jurisdiction, the applicability of the CFIUS mandatory filing rules, the risk of adverse CFIUS action, and other CFIUS-related risks to determine whether a transaction must or should be filed with CFIUS. These Layer One assessment costs are broadly distributed among the prospective investors (most of whom are based in allied countries) and among the U.S. businesses seeking

additional investment. These costs rarely prompt public expression of concern, but this assessment layer likely represents the largest locus of costs.

- Layer Two -- Process: Parties to **hundreds of transactions** each year prepare and submit CFIUS filings (after determining that their deal potentially implicates CFIUS), often with the assistance of counsel, and proceed through at least one round of review by CFIUS. Layer Two process costs sometimes prompt statements of concern to CFIUS agencies by CFIUS practitioners and parties to transactions, particularly as the time, legal fees, and uncertainty associated with the CFIUS process all have increased in the last several years; regardless, these concerns rarely lead to significant public discussion.
- Layer Three -- Mitigation: Parties to **dozens of transactions** each year are subject to mitigation measures or blocking or forced divestment. The Nippon-U.S. Steel deal is a recent and highly publicized example. Layer Three mitigation costs are more concentrated on the relevant transaction parties and sometimes prompt significant public discussion of CFIUS. The public discussion regarding the Nippon-U.S. Steel deal is an exception to the general confidentiality of the CFIUS process and was driven in part by the parties publicizing their efforts to obtain CFIUS approval for that deal.

Executive action can make each of these layers more efficient, as explained below. We prioritize recommendations within each layer after taking account of factors that include the following: (i) the extent to which the recommendation, if implemented, would improve CFIUS efficiency; (ii) the degree of consensus in favor of the recommendation among the array of CFIUS practitioners with whom we spoke; and (iii) whether CFIUS could implement the recommendation with minimal administrative rulemaking burden.

## **V. Layer One (Assessment) Recommendations**

*A. CFIUS routinely should publish anonymized covered transaction analyses.*

CFIUS only has jurisdiction over a transaction if the transaction is a “covered transaction.” If transaction parties (or counsel) conclude that there is no “covered transaction,” then they do not need to consider CFIUS further. The scope of this key term, however, is not always clear.

CFIUS should facilitate parties' ability to reach informed conclusions by publishing anonymized examples of CFIUS's own covered transaction analyses.

For decades, it has been incumbent on transaction parties to analyze whether a contemplated transaction is subject to CFIUS jurisdiction. They do so on the basis of CFIUS regulations and their own experience with CFIUS. Unlike other regulatory areas, there is negligible published precedent, as CFIUS cases generally are confidential.

CFIUS, however, conducts a "covered transaction analysis" (CTA) whenever transaction parties make a filing to CFIUS in order to determine whether the transaction falls under its jurisdiction. For CFIUS, these CTAs function as persuasive precedent for subsequent CTAs. CFIUS does not publish its CTAs, however, so parties reviewing CFIUS jurisdiction do not get the benefit of CFIUS's case-specific analyses and must rely instead on the few, limited examples published in the CFIUS regulations and the direct experiences of their counsel.

One result of this limited body of information is that there is far greater regulatory ambiguity with respect to CFIUS in general, and the parameters of a "covered transaction" in particular, than there is for key parameters in other regulatory areas (e.g., the economic threshold for Hart-Scott-Rodino antitrust filings). That ambiguity regarding CFIUS's jurisdiction, in turn, leads to additional uncertainty and higher legal fees as parties debate even whether there is a "covered transaction."

CFIUS should remedy this problem by routinely publishing anonymized CTAs, or at least those CTAs in which CFIUS addresses some ambiguity regarding the existence of a covered transaction. As with other instances of government agencies publishing adjudications of fact and law (such as Customs rulings issued by Customs and Border Protection), these would not bind CFIUS with respect to new fact patterns but would provide useful guidance to transaction parties. Doing so would require no regulatory changes and would reduce costs for thousands of transactions.

*B. CFIUS should simplify the scope of "critical technology" that can trigger mandatory CFIUS filings, particularly removing encryption items from within the scope of mandatory filing triggers.*

The scope and complexity of "critical technology" that can trigger a mandatory CFIUS filing also generates significant legal expense for thousands of transactions, very few of which pose any risk to national security. CFIUS should reduce this scope and complexity; at a minimum,

CFIUS should carve out commonplace encryption items from the scope of “critical technology” that triggers a mandatory CFIUS filing.

Determining whether a U.S. business works with “critical technology” is central to assessing whether a transaction is subject to CFIUS’ mandatory filing requirement. Most transactions filed with CFIUS are not filed because of this critical technology mandatory filing requirement but instead are filed on a voluntary basis to obtain a “safe harbor” against adverse action by CFIUS.<sup>1</sup> Nevertheless, the existence of the critical technology mandatory filing trigger obligates parties to thousands of transactions annually to determine whether they have “critical technology.” That term is defined by cross-references to hundreds of pages of technical specifications – primarily based on the Commerce Control List published under the Export Administration Regulations and the U.S. Munitions List published under the International Traffic in Arms Regulations. The scope and complexity of these specifications makes it burdensome to ascertain whether a transaction is within mandatory filing parameters.

1. Remove encryption items from the scope of critical technology that triggers a mandatory filing.

Among the most problematic features of the “critical technology” mandatory filing trigger is that it encompasses commonplace encryption items; further, due to a quirk in the way encryption is classified under U.S. export controls, encryption that is provided by a third party (e.g., Amazon Web Services) and simply used by a software product can result in the software product being considered an encryption item. Nearly every business that has proprietary software and that uses encryption – *even if that encryption is unexceptional and provided entirely by a third party* – faces a risk that its software could be classified as an encryption item and therefore within the parameters of “critical technology,” potentially making a CFIUS filing mandatory.

Although eliminating such encryption as a trigger for mandatory filing would require a change to regulations, the consensus among practitioners is overwhelmingly in favor of such a change. Few, *if any*, individuals familiar with CFIUS and related U.S. export controls believe

---

<sup>1</sup> A small subset of transactions trigger “mandatory” CFIUS filings. A far larger set of transactions is subject to CFIUS’s discretionary review authority. If a transaction is in this latter discretionary review category, the parties may make a voluntary CFIUS filing or choose to forgo a filing. Parties may choose to make a voluntary filing because, if they obtain CFIUS approval, that approval provides a “safe harbor” against adverse action by CFIUS in the future. If the parties do not make a voluntary filing, CFIUS may take adverse action at any time, including forcing divestment by a foreign investor.

that including commonplace encryption in the scope of “critical technology” mandatory filing triggers produces national security benefits; virtually all practitioners view this inclusion as an unproductive and significant burden.

2. Further simplify the scope of critical technology that triggers a mandatory CFIUS filing.

Many other practitioners have urged further simplification of the “critical technology” mandatory filing trigger but have advocated different approaches. Several practitioners suggested that CFIUS limit the scope of “critical technology” to technology regulated by the International Traffic in Arms Regulations (ITAR), the set of U.S. export control regulations focused on military technology, plus technology that is subject to certain nuclear export controls. That scope is much more easily discernible than the current, very broad and complex, “critical technology” mandatory filing parameters that include many items contained on the lengthy Commerce Control List regulated by the Export Administration Regulations. This approach would exempt many dual-use technologies from mandatory filings but retain CFIUS’ ability to scrutinize transactions involving such technologies, preserving the incentive for transaction parties in areas such as these to make voluntary filings with CFIUS.

Another practitioner suggested revisiting the North American Industrial Classification System (NAICS) Codes, which CFIUS attempted to use as part of the critical technology mandatory filing trigger in 2018-2020. Yet another practitioner suggested that CFIUS should have unfettered discretion to review any transaction involving any foreign person but that the mandatory filing rules should be eliminated because they cannot be drafted in a way that captures technology of concern and that yields mandatory filing triggers with substantial national security benefits.

In short, there was a uniform view among practitioners surveyed for this white paper that commonplace encryption should be removed from the scope of “critical technology” mandatory filing triggers and a strong consensus that the scope should be further simplified, but no consensus on the approach to that further simplification. Any meaningful simplification would require regulatory changes.

*C. CFIUS should exempt benign corporate reorganizations from mandatory filings.*

CFIUS should issue a regulation stating that no mandatory filing is triggered by a corporate

reorganization in which there are no new stakeholders and no changes to the stakes and rights of the business's owners.

This is a commonsense position and arguably implied by the fact that CFIUS, in issuing its current rules in 2020, stated that a 2008 guidance document remains in effect, and that 2008 guidance document explains that corporate reorganizations generally are not of concern to CFIUS. However, this guidance is in tension with the CFIUS mandatory filing rules, which contain no express exception for corporate reorganizations. Creating an express exception would save the significant expense of parties reviewing benign corporate reorganizations for potential mandatory CFIUS filing obligations. There is no national security benefit from U.S. businesses, foreign investors, or CFIUS spending time reviewing such corporate reorganizations.

*D. CFIUS should reduce the stringency of the “excepted investor” qualification.*

Further, there is a strong CFIUS practitioner consensus that the carve-out from mandatory filing obligations for “excepted investors” is far too complex and restrictive. Currently, investors from Australia, Canada, New Zealand, and the United Kingdom (collectively, Excepted Foreign States or EFS) can qualify as excepted investors *if they meet many other complex criteria*. For an investor, these include not only being incorporated in an EFS but also headquartering in an EFS, having 75% or more of board of directors and observers from an EFS, having all owners with 10% or greater equity from an EFS, and ensuring that a specified level of economic and voting interest (50% for a publicly traded company and 80% for a private company) is from an EFS.

Because the qualifications to be an excepted investor are many and complex, excepted investor status is rarely utilized as a basis for determining that there is no mandatory filing obligation. Rather, parties search for other bases on which to conclude that there is no mandatory filing obligation. Further, the determinative facts are subject to change over time, so the excepted investor analyses might have to be repeated in future rounds of investment, even if the investor otherwise presents substantially the same risk profile.

Many practitioners suggested that all the criteria should be loosened and that some could be jettisoned entirely – for example, that it should be sufficient if an investor is incorporated in an EFS, a controlling majority of its board is from the EFS, and the majority of its owners is from the EFS. Simplifying the EFS requirements as indicated here would require formal regulatory changes, but these changes broadly would be consistent with the Trump

Administration’s “American First Investment Policy,” which emphasizes the importance of attracting investment from allied countries.

## **VI. Layer Two (Process) Recommendations**

Whereas the recommendations above aim to reduce costs arising from obligations to determine *whether* a filing is warranted with respect to thousands of transactions per year, the Layer Two recommendations concern those several hundred transactions annually that *are* filed with CFIUS.

### *A. CFIUS should rescind the “completion date” FAQ.*

In May 2023, CFIUS posted a Q&A on the [FAQ section of the CFIUS website](#) announcing a technical change to the CFIUS definition of “completion date.” The change was that, according to the FAQ, the “completion date” of a transaction for the purposes of CFIUS review is the date on which a foreign investor obtains equity or contingent equity in the U.S. business, rather than, as previously understood, the date on which the investor receives certain critical rights in that U.S. business (e.g., when the investor receives the right to a board seat). This unusual effort to change a widely understood interpretation of a regulatory term via the informal mechanism of an FAQ is procedurally problematic – applicable law requires CFIUS to use its formal regulatory process, which requires publishing a new rule in the Federal Register and holding a public comment period. Had CFIUS followed this process, stakeholders could have alerted CFIUS to the substantive effects of the FAQ, which are significant, as described below.

Specifically, for transactions subject to mandatory CFIUS filings because they involve U.S. “critical technology,” the revised FAQ has the substantive effect of preventing foreign investors – including U.S. allies – from executing certain “passive” investments. Under applicable CFIUS regulations, minority investments (generally less than 10% voting stake) with no board seats, information access, or other special rights generally are understood as “passive” investments, reflecting CFIUS’s judgment that such investments are benign from a national security perspective, regardless of the identity of the investor. Prior to the CFIUS FAQ, it was common for investors to make passive investments with “springing rights” (e.g., the right to a board seat) that would come into existence upon CFIUS approval. The FAQ, though, prohibits such arrangements where the U.S. company has critical technology that triggers a mandatory filing. The FAQ insists that a mandatory CFIUS filing must be made 30 days before an investor obtains any equity in the U.S. company, regardless of the passive

nature of the investment, if springing rights (e.g., a board seat) will come to fruition upon CFIUS clearance.

There is no national security benefit to precluding passive investments where springing rights are conditioned on eventual CFIUS approval. Indeed, the Trump administration has emphasized that it welcomes passive investments from all foreign investors. The practical effect of the FAQ change, however, has been to raise the cost of capital for critical technology companies by deterring would-be foreign investors from investing if they cannot make passive investments quickly, with springing rights conditioned upon CFIUS approval. These critical technology companies are those whose protection CFIUS has prioritized, so it is unfortunate that CFIUS has increased capital costs for critical technology companies without any commensurate national security benefit.

The CFIUS “completion date” FAQ should be rescinded and replaced with an acknowledgment that passive investments with springing rights are permissible, consistent with prior established understandings of the term, CFIUS regulations, and the Trump administration’s welcoming of passive investments.

*B. CFIUS should designate an “Efficiency Advocate” within the Treasury Department.*

In previous decades, the Departments of the Treasury, Commerce, and State, as well as the Office of the U.S. Trade Representative – all CFIUS member agencies – often advocated in favor of approving transactions and running an efficient process, citing the U.S. government commitment to the longstanding “open investment policy” that welcomes foreign investors. However, a common view among not only CFIUS practitioners but also current and former CFIUS officials is that the weight of this norm in CFIUS deliberations has declined as national security concerns about such investments have grown, a dynamic that FIRRMA both reflects and spurs.

Consistent with that dynamic, CFIUS officials often take a skeptical view of foreign investment and are incentivized to ask searching questions to demonstrate concerns about even remote national security risk. While this is understandable and often warranted, there is a strong practitioner consensus that this too often devolves into duplicative and unproductive questions from CFIUS that impose significant costs on transaction parties. The parties must spend time and money answering questions, and the incentives for CFIUS to continue asking questions sometimes can lead to CFIUS being unable to clear a transaction within the statutory timeframe (usually ninety days from the date of the parties filing a notice

to CFIUS), contributing to the attendant dynamic in which the parties often withdraw and re-file a notice to enable CFIUS to have more time.

CFIUS therefore should designate an Efficiency Advocate – a new unit within the Treasury Department’s Office of Investment Security, which manages the CFIUS process. The Efficiency Advocate would be subordinate to the Treasury Department’s overall position in any specific case (it would not function akin to an independent inspector general).

The Efficiency Advocate should identify and resolve, for individual transactions and the CFIUS process writ large, inefficiencies across the CFIUS enterprise by promoting standardization, eliminating duplicative and unnecessary questions, and looking for other opportunities to minimize the time and expense that transaction parties incur when going through the CFIUS process. For a range of cases, a dedicated Efficiency Advocate could significantly reduce duplicative and unproductive question-and-answer sets; push CFIUS to complete a higher percentage of cases before the milestone forty-five-day marker (rather than the ninety days that has become more common); enable transaction parties and CFIUS to negotiate and conclude any necessary mitigation agreement within ninety days (rather than accepting “withdrawal and re-filing” and the “CFIUS overtime” periods that have become increasingly common); and help keep CFIUS’ focus on the national security risks presented by the transaction under discussion

To make efficiency issues more visible, the Efficiency Advocate also should prepare an annual CFIUS process efficiency report that would be separate from, and in addition to, the congressionally mandated annual CFIUS report. This efficiency report should include statistics such as how many questions were asked in the course of a CFIUS review, when the first draft of mitigation measures was circulated among CFIUS member agencies, and how long into the CFIUS process parties were initially notified of the existence of a national security concern.

No new regulations would be needed for CFIUS to designate an Efficiency Advocate.

*C. CFIUS should implement the announced “Known Investor” program*

Earlier this year, Treasury [announced](#) plans for a “Fast Track Pilot Program for Foreign Investors.” The purpose of this so-called “Known Investor” program is to encourage investment in the United States by fast-tracking some of the several hundred annual CFIUS

reviews where the investors are known to CFIUS and determined to present little or no threat to national security.

This concept has support among many CFIUS practitioners, some of whom have suggested adopting an expansive circle of potential “Known Investors.” For example, any foreign investor that received CFIUS approval in the last two years could be eligible for fast-tracking, perhaps with the default being that subsequent transactions filed with CFIUS by that foreign investor would be deemed approved within thirty days absent CFIUS concluding that additional vetting or mitigation is necessary.

One difficulty is that, when assessing national security risk, CFIUS assesses the threat presented by the investor and the sensitivity of the U.S. business in tandem. An investor that may quickly be deemed benign for the purchase of a U.S. fashion company, for example, might warrant more scrutiny for the purchase of a cybersecurity company. CFIUS could address this problem with a thirty-day approval *default* unless a senior official (e.g., a Deputy Secretary) deems the U.S. business to be sufficiently sensitive that a longer CFIUS process is needed. CFIUS also should issue guidance regarding the factors that the Deputy Secretary or other senior official must consider in the course of making any determination that the thirty-day approval default should be inapplicable.

Each of these Known Investor proposals would require rulemaking.

## **VII. Layer Three (Mitigation) Recommendations**

For transactions that CFIUS will not approve unless the parties accept risk mitigation, we have two primary recommendations, neither of which would necessarily require changes to regulations. The first recommendation is that the Deputy Secretary of each of the lead CFIUS agencies should have to certify, in writing, that the proposed mitigation measures are necessary and appropriately tailored to address the national security risks. The second recommendation is that mitigation measures and compliance processes should be standardized as much as possible; current circumstances encourage third-party monitors and auditors to fault companies for non-substantive issues, yielding results that are idiosyncratic and needlessly burdensome.

- A. *The Deputy Secretary of each lead CFIUS agency should certify in writing that mitigation is necessary and that the mitigation measures proposed by CFIUS are appropriately tailored.*

There is a consensus among CFIUS practitioners – and many CFIUS government officials acknowledge this, too – that CFIUS increasingly imposes mitigation measures on transactions as a hedge against domestic political risk, as opposed to genuine national security risk. In the current environment, CFIUS officials often worry that they will be criticized for approving a transaction, particularly if the investor has any link to China, regardless of how attenuated the link (e.g., an investor that derives some revenue from China sales). At the same time, the “open investment” norm has not completely evaporated, so blocking a transaction often is unappealing. As a result, CFIUS officials are under pressure to insist on mitigation measures that often do little for national security because the risks that the measures purport to mitigate are vanishingly remote or because the measures are not appropriately tailored to the risks.

Requiring lead agency certification at the Deputy Secretary level might, in some cases, act as a check against CFIUS staff proposing mitigation measures to address insignificant risks or proposing measures that are ill-suited to address the risks.

Further, the “necessary” and “appropriately tailored” findings should be required to impose mitigation measures beyond a five-year period – that is, mitigation agreements should include a default sunset at five years unless renewed upon a finding by Deputy Secretaries from the lead agencies.

*B. CFIUS should develop standards for monitors and auditors that focus these third parties on violations that present substantive national security risks.*

Many CFIUS mitigation agreements include measures requiring the U.S. business to hire a third-party compliance monitor and/or an auditor that reports to CFIUS about the company’s compliance record. (In the CFIUS context, a “monitor” reviews operations continually, whereas an “auditor” generally reviews on an annual or other periodic basis; for simplicity we will sometimes refer to both as auditors). CFIUS does not have the resources to scrutinize periodically every U.S. business with a mitigation agreement, so these third-party oversight measures aim to fill a gap in CFIUS’ enforcement functions.

It is [well-established](#) in the economics literature on third-party auditors in other domains that auditors often must navigate a conflict of interest. On the one hand, an auditor has an economic incentive to grow the auditing business, which requires having customers willing to pay for audits. Often, the paying customer is also the target of the audit. The auditor’s

business interests generate an incentive for the auditor to expand the scope of engagement with the paying customer and/or to seek to be hired for a future engagement by demonstrating to that paying customer that the auditor is reasonable and not unduly critical. On the other hand, if the intended audience for the audit – which in many cases is not the customer paying for the audit, but rather a regulator, business partner, or customer of the paying customer – loses confidence in the quality of the audit (e.g., if the auditor is perceived as insufficiently critical), the value of the auditor’s service declines and paying customers will be less likely to hire the auditor. In a healthy market, the auditors have a disincentive to avoid being unreasonable in an audit (because paying customers will not hire the auditor again or expand the engagement) and an incentive to generate trustworthy audit results for the intended audience.

In the CFIUS context, though, U.S. businesses subject to a mitigation agreement with third-party monitor or audit provisions generally must receive approval from CFIUS when hiring a new auditor. As a practical matter, this locks in the U.S. business as a customer of the auditor, because switching to a new auditor is potentially costly: CFIUS will want to know the reasons the U.S. business is firing the incumbent auditor and replacing it with a new one, and it is unlikely to be sympathetic to complaints about auditor overzealousness. Indeed, CFIUS might even prefer such auditors and steer business to them because CFIUS does not directly experience the costs of auditor overreach. These dynamics give audit providers the leverage to potentially expand the scope of the compliance program subject to the audit, even if the cost of proposed improvements to the U.S. business are high and the benefit to national security is marginal. Within the CFIUS bar, there is widespread agreement that auditors are incentivized to create excessive compliance costs for U.S. businesses.

We believe there is now enough accumulated experience and practice to inform development of common professional standards and expectations for third-party monitors and auditors of CFIUS mitigation agreements. CFIUS should initiate a process with auditors, third-party monitors, the CFIUS bar, and other stakeholders to collaboratively develop professional standards that fulfill the national security objectives of third-party oversight.

\*\*\*\*\*

Notably, all of the nine efficiency recommendations above are consistent with the Trump administration’s policy objectives and can be implemented without legislation – and, for many of the recommendations, without undertaking any administrative rulemaking process.

## **Acknowledgements**

This paper benefited enormously from consultations with and feedback from senior CFIUS lawyers in bilateral discussions and a workshop hosted by the Stanford Program on Geopolitics, Technology, and Governance in June 2025. The authors thank Shawn Cooley, Brian Egan, Benjamin Joseloff, Christopher Kimball, Paul Marquardt, Britt Mosman, and the other practitioners who shared their comments, critiques, and insights. All views, errors, and omissions are the authors' alone.