CFIUS AND A.I.: DEFENDING NATIONAL SECURITY WHILE ALLOWING FOREIGN INVESTMENT

Theodore Bruckbauer*

CITE AS: 4 GEO. L. TECH. REV. 279 (2019)

TABLE OF CONTENTS

* J.D., Northwestern Pritzker School of Law, 2019; M.B.A., Kellogg School of Management at Northwestern, 2019; BPhil, Northwestern School of Continuing Studies, 2013. I would like to thank my wife, Kirsten, for her wisdom and partnership throughout my academic pursuits, and our son, Evan, for always finding time in my schedule to play. I extend my gratitude to the Georgetown Law Technology Review and its editors for graciously facilitating the publication of this note.

I. INTRODUCTION

Artificial intelligence is one of the most important innovations to impact national security in recent years.[1] Among the national security concerns of the United States is that foreign countries seek to erode America's leadership in artificial intelligence development by buying or merging with U.S. companies.[2] In response to this perceived threat, Congress passed legislation in 2018 to expand the authority of the Committee on Foreign Investment in the United States (CFIUS).[3] CFIUS conducts reviews for national security concerns on certain transactions where a foreign-controlled entity aims to acquire a stake in a U.S.-based company.[4] If national security concerns are not resolved during its review, CFIUS may recommend the President block the transaction.[5]

For foreign companies that pose perceived threats to national security, an important part of the CFIUS review process is mitigations—binding agreements between CFIUS and the transacting companies that resolve security concerns and allow the transaction to receive approval. Foreign companies with proposed investments in U.S. artificial intelligence that could be perceived to threaten national security should expect CFIUS to approve transactions only after mitigations are in place. Those companies must therefore understand the unique national security concerns posed by artificial intelligence and which mitigations might resolve them. This paper seeks to provide that guidance.

Part II of this paper provides an overview of CFIUS and its review process. It explains the stages of CFIUS review and places mitigations inside this larger context. Part III introduces the 2018 legislation that targeted artificial intelligence transactions and reviews its legislative history. Part IV is devoted to mitigations. It first assesses the usefulness of traditional mitigations in artificial intelligence transactions and then recommends sources to aid in development of new categories of mitigations.

[1] *See generally* DANIEL S. HOADLEY & KELLEY M. SAYLER, CONG. RESEARCH SERV., R45178, ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY (2019) [hereinafter CRS AI & NATIONAL SECURITY REPORT].

[2] *See* Paul Mozur & John Markoff, *Is China Outsmarting America in A.I.?*, N.Y. TIMES (May 27, 2017), https://www.nytimes.com/2017/05/27/technology/china-us-ai-artificial-intelligence.html [https://perma.cc/4MFJ-GHAA].

[3] JAMES K. JACKSON, CONG. RESEARCH SERV., IF10952, IN FOCUS: CFIUS REFORM: FOREIGN INVESTMENT NATIONAL SECURITY REVIEWS 1 (2018).

[4] JAMES K. JACKSON, CONG. RESEARCH SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 1 (2018) [hereinafter CRS CFIUS REPORT].

[5] *Id.* at 13.

II. CFIUS BACKGROUND AND PROCESS

A brief history and description of CFIUS, its purpose, and the CFIUS review process provide context for subsequent discussions of recent changes in the review process.

A. CFIUS Background

The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee that serves the President in overseeing the national security implications of foreign direct investment (FDI) in the U.S. economy.[6] It consists of nine mostly Cabinet-level officials, including the Secretaries of State, the Treasury, Defense, Homeland Security, Commerce, and Energy; the Attorney General; the United States Trade Representative; and the Director of the Office of Science and Technology Policy.[7] The Secretary of Labor and the Director of National Intelligence serve as ex officio members of the Committee.[8] President Gerald Ford established the Committee in a 1975 Executive Order and granted to it "primary continuing responsibility within the Executive Branch for monitoring the impact of foreign investment in the United States."[9] Among other responsibilities, the Order instructed the Committee to review investments which "might have major implications for United States national interests."[10] President Ford created the Committee to encourage foreign investment and "dissuade Congress from enacting new restrictions."[11]

In 1988, the Exon–Florio Amendment to the Defense Production Act ("Exon–Florio") codified the process CFIUS used to review foreign investment transactions.[12] Importantly, Exon–Florio also granted power to the President to block mergers, acquisitions, and takeovers that threaten to impair national security. The Amendment grants this authority whenever the President has "credible evidence" that the investment will impair national security and no other U.S. laws adequately protect U.S. security interests.[13]

A contemporaneous Executive Order delegated the President's power to conduct reviews, undertake investigations, and make recommendations to

[6] *Id.* at 1.

[7] *Id.* at 14.

[8] *Id.*

[9] Exec. Order No. 11858, 3 C.F.R. § 990 (1971–1975).

[10] *Id.*

[11] *The Operations of Federal Agencies in Monitoring, Reporting on, and Analyzing Foreign Investments in the United States: Hearings Before the Subcomm. on Commerce, Consumer, and Monetary Affairs*, 96th Cong. 334–335 (1979).

[12] CRS CFIUS REPORT, *supra* note 4, at 6.

[13] *Id.* at 7.

CFIUS.[14] Thus, CFIUS now performs investigations and makes recommendations to the President when it believes a transaction should be blocked. The 1992 Byrd Amendment to the Defense Production Act went on to mandate reviews whenever a foreign acquirer acts on behalf of a foreign government.[15]

2007 brought a major update to CFIUS through the Foreign Investment and National Security Act of 2007 (FINSA).[16] FINSA codified CFIUS's position in the review and recommendation process and increased the number of factors the President could consider in making a decision.[17] It also required high-level CFIUS members to certify to Congress that no unresolved national security issues exist in reviewed transactions.[18] Certification must be made by a person ranking no lower than Assistant Secretary level for reviewed transactions and Secretary or Deputy Secretary level for investigated transactions.[19]

The next major update to CFIUS took place in 2018.[20] The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) was passed as part of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.[21] FIRRMA made numerous changes that expanded the scope of transactions that fall under CFIUS's review by redefining "covered transactions" to include joint ventures and noncontrolling investments in critical—and emerging—technology companies.[22] Additionally, FIRRMA mandates filing of certain transactions with CFIUS.[23] These changes were put in effect through a Treasury Department pilot program on November 10, 2018.[24]

B. CFIUS Review Process

The CFIUS review process is comprised of one informal step and three formal steps.[25] The informal step is one of indefinite length during which

[14] *Id.* at 6.

[15] *Id.*

[16] Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246 (codified as amended in scattered sections of 50 U.S.C.).

[17] CRS CFIUS REPORT, *supra* note 4, at 12, 14.

[18] *Id.* at 14.

[19] *Id.*

[20] JAMES K. JACKSON, CONG. RESEARCH SERV., IF10177, IN FOCUS: THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES 1 (2019) [hereinafter CRS IN FOCUS: CFIUS].

[21] CRS CFIUS Report, *supra* note 4, at 11.

[22] CRS IN FOCUS: CFIUS, *supra* note 20, at 2.

[23] *Id.*

[24] CRS CFIUS REPORT, *supra* note 4, at 18.

[25] *Id.* at 10.

transactions that will potentially require a formal investigation are screened.[26] During this phase, firms considering foreign direct investment work with CFIUS to identify potential issues prior to the beginning of an investigation.[27] This period allows firms to address issues that might be raised before risking any negative publicity that might accrue if the transaction is blocked on national security grounds.[28]

A transaction enters the formal review process when the transacting companies notify CFIUS of their proposed transaction or when CFIUS initiates a review. In the past, many transacting companies entered the formal review process willingly by notifying CFIUS of their proposed investment, merger, or acquisition.[29] Firms subjected themselves to scrutiny because transactions completed without CFIUS review are subject to forced divestment by the President at any time in the future.[30] With the passage of FIRRMA and corresponding regulations, the filing of transactions with CFIUS became mandatory for foreign investments in U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies.[31] Some lower risk transactions will, however, benefit from a new expedited review process that forgoes a formal review.[32] In addition to the parties to an investment transaction, any member of CFIUS or the President may initiate a formal review of that transaction.[33]

Once a transaction reaches the formal review process, the process can proceed potentially through three steps: (1) the National Security Review, (2) the National Security Investigation, and (3) Presidential Determination.[34] At each step, CFIUS members weigh factors and work with the transacting companies to identify security concerns and attempt to clear the transaction.[35] CFIUS can grant approval at either of the first two formal steps and the President can approve or block a transaction at step three.[36]

The first formal step is the National Security Review. During this step, CFIUS is required to conduct a review if the investment threatens to impair national or homeland security, critical infrastructure, or critical technologies; and the transaction would result in foreign control of a U.S. entity.[37] The

[26] *Id.* at 12.

[27] *Id.* at 11.

[28] *Id.*

[29] CRS IN FOCUS: CFIUS, *supra* note 20, at 1.

[30] *Id.*

[31] CRS CFIUS REPORT, *supra* note 4, at 17.

[32] *Id.*

[33] CRS CFIUS REPORT, *supra* note 4, at 12.

[34] CRS IN FOCUS: CFIUS, *supra* note 20, at 1.

[35] *Id.*

[36] *Id.*

[37] *Id.*

Director of National Intelligence, an ex officio member of CFIUS, reviews the national security implications of the foreign investment and CFIUS assesses the impact of the investment using factors enumerated by Congress.[38] The Secretary of the Treasury may unilaterally exempt a transaction from the process at this stage if he or she determines the transaction will not impair security.[39]

The second step is the National Security Investigation. CFIUS launches an Investigation if any of its members determine during the first step that the transaction threatens to impair national security.[40] The second step is a more thorough review of the national security implications of allowing the transaction to proceed. Critically, this phase allows CFIUS and the parties to the transaction to agree to mitigations.

CFIUS can negotiate, enter into, impose, and enforce "any agreement or condition with any party to the covered transaction in order to mitigate any risk to the national security of the United States that arises as a result of the covered transaction."[41] Details of agreed upon mitigations are generally not public. CFIUS, however, includes a high-level list of mitigations used during a calendar year in its annual report to Congress. The list is largely static from year-to-year which suggests that many mitigations are commonly used. Section IV below discusses mitigations in detail.

The final step is Presidential Determination. If the transacting parties and CFIUS cannot agree on mitigations, CFIUS can recommend that the President suspend or block the transaction.[42] The Office of the President has used its authority to block only five transactions under this legal regime.[43] The rarity of this action suggests that most companies either agree to mitigations or withdraw once CFIUS intends to recommend Presidential intervention.

In summary, companies proposing transactions that implicate national security are funneled into a process where they must negotiate mitigations that relieve national security concerns or back out of the transaction (independently or by Presidential action). For these companies, finding effective mitigations during the National Security Investigation (or sooner) is key to successful CFIUS approval.

[38] *Id.*

[39] CRS IN FOCUS: CFIUS, *supra* note 20, at 1.

[40] *Id.*

[41] 50 U.S.C. § 4565(l)(3)(A)(i) (2018).

[42] CRS CFIUS REPORT, *supra* note 4, at 13.

[43] *Id.* at 7.

III. FIRRMA AND THE IMPLICATION OF ARTIFICIAL INTELLIGENCE

The expanded powers of CFIUS and legislative history of FIRRMA show the legislative concerns that led to CFIUS's expansion.

A. Overview

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) expanded the role of CFIUS.[44] FIRRMA redefined "covered transactions" to include joint ventures and noncontrolling investment in critical and emerging technology companies.[45] It also made filing with CFIUS mandatory for certain transactions, lengthened the review periods, and provided CFIUS with additional funding and staff.[46] The broad changes appear to have a narrow focus—capture strategic investments by foreign countries in emerging technology companies and give CFIUS the tools to review them thoroughly. Despite there being no mention of artificial intelligence within the text of FIRRMA, the analysis below demonstrates that foreign investment in artificial intelligence companies is Congress' primary concern.

B. Legislative History and Support

An emerging consensus in the government that artificial intelligence is a critical emerging technology and requires protection led to FIRRMA's implementation and usage. In a 2017 hearing before the Senate Committee on Banking, Housing, and Urban Affairs, the Senate Committee and witnesses discussed a report drafted by the Defense Innovation Unit Experimental (DIUx)[47] about China's technology acquisition strategy.[48] The report provided data and arguments which serve to support FIRRMA.[49] The main findings of

[44] CRS IN FOCUS: CFIUS, *supra* note 20, at 2.

[45] *Id.*

[46] *Id.*

[47] The Defense Innovation Unit Experimental (DIUx), now DIU, is an entity, founded by the Department of Defense, that invests in private sector companies to solve national security issues. *See* Billy Mitchel, *'No longer an experiment'—DIUx Becomes DIU, Permanent Pentagon Unit*, FEDSCOOP (Aug. 9, 2018), https://www.fedscoop.com/diu-permanent-no-longer-an-experiment/ [https://perma.cc/ETB7-534H].

[48] *Examining The Role Of The Committee On Foreign Investment In The United State: Hearing Before the Subcomm. On Monetary Policy & Trade of the H. Comm. On Fin. Servs.*, 115th Cong. 28 (2017).

[49] *See* MICHAEL BROWN & PAVNEET SINGH, DEF. INNOVATION UNIT EXPERIMENTAL, CHINA'S TECHNOLOGY TRANSFER STRATEGY: HOW CHINESE INVESTMENTS IN EMERGING TECHNOLOGY ENABLE A STRATEGIC COMPETITOR TO ACCESS THE CROWN JEWELS OF U.S. INNOVATION (2018).

the report were that Chinese investments in venture-backed startups were at record levels and growing rapidly.[50] Additionally, the report found that the technologies targeted by these investments are the same ones where U.S. firms are investing and will be foundational to future innovations.[51] The report recommends expanding the role of CFIUS to counter these trends.[52] The technology discussed most prominently in the report and hearing is artificial intelligence.

Both houses of Congress introduced FIRRMA bills on November 8, 2017.[53] The House reintroduced a FIRRMA bill on May 16, 2018, where it passed with a vote of four hundred to two.[54] A final version became law as part of Title XVII of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.[55]

Another example of Congress' concern with foreign investment in U.S. artificial intelligence appeared as Title X of the same act. Title X created the National Security Commission on Artificial Intelligence to review, *inter alia,* "[d]evelopments and trends in international cooperation and competitiveness, including foreign investments in artificial intelligence, related machine learning, and computer science fields that are materially related to national security and defense."[56]

President Trump joined Congress in his support for using CFIUS to regulate artificial intelligence transactions. In 2017, he followed a recommendation from CFIUS and blocked the foreign acquisition of Lattice Semiconductor, a company that manufactures chips critical to artificial intelligence development.[57] In 2018, he voiced support for the idea of using CFIUS to protect technology developed by Silicon Valley.[58] Finally, in 2019, President Trump issued an Executive Order that encouraged concerted efforts to protect America's leadership in artificial intelligence.[59]

[50] *Id.* at 5.

[51] *Id.* at 2.

[52] *Id.*

[53] Foreign Investment Review and Modernization Act of 2017, H.R. 4311, 115th Cong. (2017); Foreign Investment Risk Review Modernization Act of 2017, S. 2098, 115th Cong. (2017).

[54] 164 CONG. REC. H4137 (daily ed., May 16, 2018) (introduction of H.R. 5841 by Rep. Robert Pittnger).

[55] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018).

[56] *Id.* § 1051(b)(2)(C).

[57] CRS AI & NATIONAL SECURITY REPORT, *supra* note 1, at 7.

[58] *See* Shawn Donnan, *Donald Trump Softens Tone on Chinese Investments*, FIN. TIMES (Jun. 26, 2018) https://www.ft.com/content/3ce53380-798f-11e8-bc55-50daf11b720d [https://perma.cc/Y7CT-D7T9].

[59] Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 11, 2019).

Together, these actions point to a broad consensus in the government that artificial intelligence is a critical emerging technology that requires protection. Congress intends CFIUS to provide that protection and passed FIRRMA to ensure the Committee has the authority and resources needed to do so. With review of artificial intelligence transactions certain to become the norm, CFIUS and transacting companies must now learn to mitigate the security risks that arise from such transactions.

IV. MITIGATION MEASURES

This section describes mitigations and their place in the CFIUS approval process, discusses how traditional mitigations may be applied to artificial intelligence transactions, and suggests sources for new mitigations that address the unique traits of artificial intelligence.

A. Description & Purpose

Mitigations are binding agreements between CFIUS members and the transacting companies that resolve security concerns to allow transaction approval. CFIUS's declassified yearly report includes a bullet-point list of mitigation measures "negotiated and adopted" that "required the businesses involved to take specific and verifiable actions."[60] For foreign companies that pose perceived threats to national security, negotiated mitigations are perhaps the most important step in the CFIUS process. When the Committee determines national security concerns exist, mitigations are required before transaction approval. Without mitigations, the only path to approval in these cases is by presidential ruling against the advice of the Committee.

As already noted, the mitigations are negotiated between the transacting companies and CFIUS. Neither side has dictatorial control of the terms. Instead, CFIUS looks to reach an agreement that meets an acceptable security standard and the companies try to accommodate that standard at minimal cost to themselves. From 2013 to 2015, forty cases resulted in the use of legally binding mitigation measures.[61] But, finding workable mitigations is by no means guaranteed. In 2015, at least three transactions were abandoned after CFIUS and the parties could not identify acceptable mitigations.[62]

CFIUS does not publicly divulge the national security concerns that lead to the introduction of mitigations into the review of a transaction. Thus, an understanding of CFIUS's intent must be extracted from the mitigations themselves. A pragmatic interpretation is useful here and will reveal three

[60] COMM. FOREIGN INVEST. U.S., ANNUAL REPORT TO CONGRESS (CY 2015) 21 (2017).

[61] *Id.*

[62] *Id.* at 20.

traits about mitigations. First, each mitigation alludes to one or more concern CFIUS has with a transaction. If there were no corresponding concern, there would be no cause for the mitigation to exist. Second, CFIUS views the mitigation as acceptably resolving the concern or it would not have approved it. Finally, the imposed control is not so onerous on the companies or so material to the transaction that the parties prefer to abandon the transaction instead of agreeing. In other words, the inclusion in the annual report of a mitigation shows that at least some companies accepted the mitigation and its associated costs.

These three traits are demonstrated in an example of a mitigation from a recent CFIUS report: that the business must "[n]otify security officers or relevant [U.S. Government] parties in advance of foreign national visits to the U.S. business for approval."[63] First, this mitigation reveals CFIUS's concern about access to domestically located secrets of the U.S. company by foreign nationals. Second, it reveals that vetting foreign visitors resolves that concern. Lastly, agreement to this mitigation by the transacting companies shows that getting pre-approval for foreign visitors is not an overly large burden, perhaps because it is an infrequent occurrence within these companies.

This understanding of the purpose and interpretation of mitigations makes it possible to evaluate how traditionally used mitigations might be used in future artificial intelligence transactions.

B. Traditional Mitigations as They Pertain to Artificial Intelligence

This section will address how traditional mitigations commonly found in CFIUS reports—integrity assurance, exclusion of sensitive assets from transactions, and access restrictions—can be applied to artificial intelligence. While these mitigations could be used in transactions dealing with artificial intelligence and national security, issues unique to artificial intelligence pose problems in applying these traditional mitigations.

1. *Integrity Assurance*

Of the previously used mitigations, the only to mention software is integrity assurance: "[s]ecurity protocols to ensure the integrity of goods or software sold to the [U.S. Government]."[64] Though CFIUS does not list the specific concerns that spawned a mitigation, this mitigation is likely designed to address a concern that a foreign controlled company that provides software may make dangerous or undesirable changes without the U.S. government's detection.

[63] *Id.* at 21.

[64] *Id.*

A scenario leading to this mitigation is easy to imagine. For example, a national security concern would arise if an untrusted foreign company acquired a U.S. software company that develops software for the U.S. government. The software might be custom and application specific—such as code for weapons systems—but could also be mundane business software, like word processors or spreadsheet software. In either case, there is a risk that foreign actors in control of strategic software development could make changes, malicious or otherwise, that have adverse effects. Both intentionally and inadvertently introduced vulnerabilities can compromise the integrity of mission-critical software.

Principles used to protect the integrity of traditional software are transferable to artificial intelligence software, with one notable exception. Where traditional software is expected to be deterministic (i.e. it returns the same correct output for each possible input), artificial intelligence is useful because of its efficacy at tasks that cannot be described by deterministic rules.[65] Furthermore, correctly functioning artificial intelligence systems always display some rate of error.[66] Because of these traits, a method of integrity assurance other than testing inputs and outputs is required.

One possible solution to this problem would be limiting changes to the software's development. If the U.S. government trusts software prior to a foreign acquisition, it must believe that the development process will not create unwanted changes. For that trust to continue after an acquisition, that process must be protected. This type of integrity assurance might be possible, but it has three limitations.

First, even the strictest agreement to protect the development process may not satisfy CFIUS. Bias introduced intentionally or unintentionally might result from new or different programmers, training data, preferences for different statistical models, or tuning decisions. Bias in artificial intelligence can be extremely hard to detect.[67] Without extreme controls, CFIUS may not view development protections as adequate.

Second, introducing controls that meet CFIUS's standards may be too costly for the parties to the transaction. Monitoring becomes more costly as the number of decisions under scrutiny increases. At some level of granularity, the cost of monitoring will outweigh the value of the project. Said another

[65] HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, EUR. COMM., A DEFINITION OF AI: MAIN CAPABILITIES AND DISCIPLINES 3–5 (2019).

[66] *Id.* at 4.

[67] *See* Jeremy Kun, *Big Data Algorithms Can Discriminate, And It's Not Clear What To Do About It*, THE CONVERSATION (Aug. 13, 2015) http://theconversation.com/big-data-algorithms-can-discriminate-and-its-not-clear-what-to-do-about-it-45849 [https://perma.cc/5HSP-P5FL].

way, it might be so expensive to appease CFIUS that companies may choose to withdraw from the transaction rather than agree to the controls.

Finally, any controls might materially reduce the value of the acquired artificial intelligence if they prevent future development or new uses. Unlike the above point, the controls do not need to be extreme to have an effect. Even inexpensive controls, such as limiting training data to a trusted source, might create a competitive disadvantage against others operating without similar limitations. Limitations that greatly reduce the value of a targeted company's technology will cause acquirers to abandon transactions.

In conclusion, non-deterministic outputs, the risk of undetectable bias, and costs arising from development controls make it unlikely that CFIUS and transacting companies will find workable mitigations based on integrity assurance.

2. *Exclusion of Sensitive Assets from the Transaction*

Another mitigation that appears in the annual reports is the "exclusion of sensitive assets from the transaction."[68] Interestingly, the use of this mitigation shows that companies are willing to complete at least some transactions even when the most sensitive technologies of the acquired company are withheld and sold to third parties.

Machine learning, a form of artificial intelligence, is a combination of statistical models and processes encoded in software, trained on data, often with manual refinements and tuning made after deployment.[69] Any one of these components might on its own be considered too sensitive to sell to a foreign power. For example, CFIUS might decide that the data underlying the models is too sensitive but the models themselves are uncontroversial, or precisely the opposite. It is also possible that isolating a single component of concern is not possible: some artificial intelligence may be more than the "sum of its parts."

This difficulty can be illustrated with two examples. First, consider a hypothetical case where an artificial intelligence is part of a larger system: a company that gives conventional missiles devastatingly effective results through the inclusion of custom artificial intelligence targeting software. If a foreign entity attempted to buy this company, CFIUS might insist on excluding the artificial intelligence software over concerns it be used against the United States. Assuming the buyer only values the capabilities of a complete system, they are unlikely to agree to this limitation. Where artificial

[68] COMM. FOREIGN INVEST. U.S., *supra* note 60, at 22.

[69] *Data Science and Machine Learning*, IBM, https://www.ibm.com/analytics/machine-learning (accessed Nov. 1, 2019) [https://perma.cc/6R34-9ZMG].

intelligence is a critical part of a system, attempts to exclude it from the transaction will lead companies to abandon otherwise viable transactions.

Second, consider the case where a U.S. company makes only general-purpose artificial intelligence and does not produce a product with identifiable sensitive components or with readily apparent uses. How might CFIUS attempt to judge the threat posed by a foreign acquisition in this case? One option is to attempt to predict potential uses of the acquired technology to block transactions that pose a future threat. It seems unlikely, however, that these predictions will form a reliable basis for CFIUS intervention. Alternatively, CFIUS might attempt to block transactions involving technology so advanced that it is *de facto* sensitive regardless of its potential uses. Aside from the difficultly in making such a determination, this method potentially projects that the United States only allows foreign investment in sub-par technologies. It is unclear how this might be resolved.

These two cases show the challenges with trying to mitigate transactions by excluding all or part of a company's artificial intelligence assets. The barriers present in the sale of stand-alone artificial intelligence technology and those present in the sale of integrated artificial intelligence systems will often occur together, further complicating the conversation. Where artificial intelligence is material to the transaction, any attempt to exclude it either wholly or in-part is likely to adversely affect transactions.

3. *Access Restrictions*

Several of the mitigations listed in CFIUS's annual reports revolve around the concept of limiting untrusted parties' access to sensitive technology, products, and services.[70] Specifically, these mitigations require "[e]nsuring that only authorized persons have access to certain technology;" "[e]nsuring that only U.S. citizens handle certain products and services, and ensuring that certain activities and products are located only in the [U.S.];" and "[n]otifying security officers or relevant [U.S. Government] parties in advance of foreign national visits to the U.S. business for approval."[71] Collectively, these mitigations show that some negotiated approvals resulted in companies erecting screens between sensitive information and non-U.S. personnel.

Limiting untrusted parties' access to sensitive technology limits their ability to tamper with the technology and their ability to capture and transfer

[70] *See, e.g.,* COMM. FOREIGN INVEST. U.S., ANNUAL REPORT TO CONGRESS (CY 2012) 18 (2013); COMM. FOREIGN INVEST. U.S., ANNUAL REPORT TO CONGRESS (CY 2013) 20 (2015); COMM. FOREIGN INVEST. U.S., ANNUAL REPORT TO CONGRESS (CY 2014) 21 (2016); COMM. FOREIGN INVEST. U.S., *supra* note 60.

[71] COMM. FOREIGN INVEST. U.S., *supra* note 60.

the technology. In other words, access restrictions are alternative means to achieve some of the objectives outlined in Sections IV.B.1 and IV.B.2 above. However, unlike the previously mentioned integrity assurance or exclusion mitigations, access restrictions achieve different outcomes by targeting people rather than processes or assets.

Applying access restrictions to protect integrity is different than assuring integrity. When only trusted individuals influence the creation process, the end-product should be trustworthy, even if not verifiably so. That logic does not foreclose the usefulness of integrity assurance, but properly implemented restrictions may obviate it to some degree.

Conversely, access restrictions to prevent loss of sensitive technology to foreign adversaries is a mirror image of asset exclusion. Instead of excluding the assets from the transaction, the people are excluded. It would not make sense to have both regarding the same piece of technology.

4. *Access Restrictions Compared to Other Mitigations*

Comparing the effectiveness of the above mitigations as applied to artificial intelligence, access restriction mitigations are more appropriate and effective than the assurance and exclusion mitigations, as four unsolved issues that arise from integrity assurance and asset exclusion can be partially resolved through access restrictions.

The first issue with integrity assurance raised in Section IV.B.1 is that it may be impossible to reduce unwanted foreign influence on development enough to satisfy the integrity demands of CFIUS. This is because even small interactions might introduce an undetectable bias. The desired reduction in foreign influence may be accomplished by altogether removing access. Access restrictions have a distinct advantage over assurance because it preempts any opportunity for bias or tampering to seep in.

The second issue raised with integrity assurance, that the cost of monitoring the development of artificial intelligence systems might be too high, is another situation in which access restrictions have a distinct advantage. A system that approves clearance for known personnel is more efficient than oversight of individual design choices; it is also easier to enforce and audit.

The third issue with integrity assurance is that even minimal controls might materially affect the value of the acquired technology. Section 1 noted that artificial intelligence might develop less competitively under method or data limitations. Likewise, artificial intelligence will develop less efficiently if access restrictions prevent access by highly skilled but foreign data scientists. Access restrictions, however, may target persons other than the scientists and developers. It is therefore possible that some restrictions would satisfy CFIUS's national security concerns without negatively impacting development.

Lastly, access restrictions may be more effective than exclusion mitigations. Section IV.B.2 discusses attempts to protect sensitive artificial intelligence from foreign ownership by excluding it in whole or in-part from transactions and concludes that there may be insurmountable problems with that approach. As in Section 2, it is necessary in restricting access to evaluate artificial intelligence by its individual subcomponents, and thus the difficulty of isolating components of concern remains. However, if CFIUS successfully isolates the sensitive components, access restrictions work better than asset exclusion.

Section 2 argued that a buyer who values the capabilities of a complete system where artificial intelligence is a critical piece would object to a mitigation that removes the artificial intelligence from the transaction. Access restrictions do not raise the same concern because they allow the complete system to remain intact. They therefore create a possible avenue to acceptable mitigations in scenarios where CFIUS's concerns can be addressed by, for example, limiting access to U.S. citizens.

Overall, access restrictions might be more appropriate for artificial intelligence transactions than either integrity assurance or asset exclusion. Though they do not resolve all issues, access restrictions are more appropriate when a system is holistic and hard to segment into discrete components.

C. Need for New Mitigation Options

While the mitigations revealed in the CFIUS annual reports largely remain static from year to year, new mitigations could—and should—be used if the circumstance requires. The above discussion illuminates both the failure of traditional mitigations and some of the unique traits of artificial intelligence that make it difficult to police either during development or after deployment. The non-deterministic outputs and injection of bias described in Section IV.B.1 and the difficulty of locating the specific components that drive outcomes described in Section IV.B.2 create issues for traditional mitigations.

These difficult-to-manage traits exist in all artificial intelligence systems and are not limited to those under CFIUS’s scrutiny. Commenters have raised concerns around discrimination from bias, protection of Fourth Amendment rights in the face of unexplainable algorithms, and the impact on Due Process of inaccurate artificial intelligence.[72] The solutions presented to

[72] *See, e.g.*, David Lehr and Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn about Machine Learning*, 51 U.C.D. L. REV. 653, 658, 662, 664, 703-705 (2017) (discussing current legal scholarship regarding automated suspicion algorithms and the Fourth Amendment, due process for automated predictions, and the disparate impact of big data).

these problems, though discussed as accountable or ethical principles[73] or guidelines,[74] may represent the foundation of a new class of mitigations for transactions.

In forming new principled mitigations, CFIUS and transacting companies should consider two objectives from an ethical framework to guide new families of mitigations that address artificial intelligence and national security. The first is artificial intelligence robustness assurances.

A robust artificial intelligence makes decisions that are both accurate and reproducible.[75] Accuracy pertains both to a system's ability to make correct judgments and to its ability to display an error rate lower than a predetermined acceptable level.[76] Error rates are useful because, unlike in traditional software, it is not always possible to explain why an artificial intelligence system generated a particular output.[77] This means that testing an artificial intelligence system can reveal the frequency of errors but not always the cause. Closely related to accuracy is reproducibility. An artificial intelligence system that displays perfect reproducibility generates matching outputs in initial and subsequent runs while inputs remain the same.[78] An input pattern that always causes an undesirable or incorrect output, for example, can be documented even though it remains unclear why the system acts undesirably in the particular circumstance. Together, accuracy and reproducibility describe a system's ability to meet objectives, the rate at which it does so, and the conditions under which it succeeds and fails. Robustness assurance mitigations that impose high accuracy targets, low error rate limits, and require reproducible results can be enforced and will therefore help ensure developers proceed conservatively and test to stay within compliance boundaries.

A second class of objectives to consider are artificial intelligence transparency assurances. To assure transparency, companies should adopt (or be required to adopt by CFIUS) audit-friendly practices, including explainability and traceability. Explainability is the ability for the developer or deployer to explain decisions made by the artificial intelligence to an outside auditor.[79] Traceability is the ability to follow a trail backwards to the

[73] *See Principles for Accountable Algorithms and a Social Impact Statement for Algorithms*, FAT/ML, http://www.fatml.org/resources/principles-for-accountable-algorithms (accessed Nov. 1, 2019) [https://perma.cc/VB98-P6Y9].

[74] *See* HIGH-LEVEL EXPERT GROUP AI, EUR. COMM., ETHICS GUIDELINES FOR TRUSTWORTHY AI (2019).

[75] *Id.* at 17.

[76] *Id.*

[77] *Id.* at 13.

[78] *Id.* at 17.

[79] *Id.* at 18.

root of the decision.[80] An artificial intelligence system developed in accordance with these objectives would be easier to investigate if its integrity was questioned. The traits of explainability and traceability also aid the use of access restrictions by helping to isolate sensitive components.

These two families of objectives are merely examples of the kinds of mitigations that CFIUS might derive from existing frameworks for ethical artificial intelligence. Ethical frameworks address problems caused by artificial intelligence's unique characteristics and can aid CFIUS and artificial intelligence companies in doing the same.

V. CONCLUSION

As foreign investment into U.S. artificial intelligence companies continues to rise, so will the national security concerns it brings. Congress granted CFIUS new and expansive powers to push back against investments that have the potential to undermine national security. For artificial intelligence companies courting foreign investment and for foreign investors looking to acquire U.S. know-how, the stakes have been raised. Furthermore, when artificial intelligence transactions raise national security concerns, CFIUS must identify new mitigations to cope with the unique difficulties posed by the new technology. CFIUS and transacting companies should look to existing ethical, accountable, and accuracy frameworks to create a new family of mitigations that addresses the unique characteristics of artificial intelligence.

[80] *Id.*