Discussions with the Chinese about addressing their demands have been a major part of negotiations on a bilateral investment treaty (BIT), but as of September 2015, progress on the issue has stalled despite efforts to complete agreement at the time of the visit of President Xi Jinping to Washington and Seattle. It has become increasingly apparent that the United States is not prepared to change CFIUS’s substantive procedures as China wants.

Can China nonetheless achieve much of what its investors want? Yes, almost certainly so. This Policy Brief proposes practical steps to address the concerns of Chinese investors without diluting CFIUS procedures. It provides a national security threat assessment filter, which allows Chinese investors—like investors of all nationalities—to determine when their proposed acquisitions might pose a genuine threat and when any such threat is simply not plausible. It also illustrates how foreign investors can overcome the secrecy surrounding CFIUS objections so as to figure out how to proceed with problematic acquisitions.

For more than a decade, China has complained about what it maintains has been a pattern of erratic and politicized treatment of Chinese investors when they attempt to acquire US companies. Chinese authorities remain stung in particular by the political backlash in Washington provoked in 2005 when the China National Offshore Oil Corporation (CNOOC) attempted unsuccessfully to acquire the American oil company Unocal. Although the deal was aborted by politics, and not any official finding of security concerns, the Chinese have targeted the Committee on Foreign Investment in the United States (CFIUS) as a focus of their criticism. The Chinese want the committee, an interagency group that reviews foreign acquisitions of US companies for possible threats to the national security of the United States, to be more open and transparent in its rulings and to not discriminate against Chinese firms but instead treat Chinese acquisitions on an equal basis in comparison with acquisitions by firms of other nationalities.

The United States is not likely to accede to the Chinese demands in any formal or legal manner. In a world of geopolitical tensions, acquisitions by firms from potential adversary countries will inevitably receive disproportionately intense scrutiny. Assessments by US intelligence agencies will remain secret so as not to reveal “sources and methods.”

This Policy Brief proposes practical steps to address the concerns of Chinese investors without diluting CFIUS procedures. It provides a national security threat assessment filter, which allows Chinese investors—like investors of all nationalities—to determine when their proposed acquisitions might pose a genuine threat and when any such threat is simply not plausible. It also illustrates how foreign investors can overcome the secrecy surrounding CFIUS objections so as to figure out how to proceed with problematic acquisitions.

Chinese foreign direct investment (FDI) flows in the United States have been rising rapidly since 2012, and—as this Policy Brief shows—can be expected to accelerate in the future.

It is time for an updated and revised perspective on how the CFIUS process has changed in recent years, especially with the passage of the Foreign Investment and National Security Act (FINSA) in 2009.

While CFIUS practices will not be modified to meet Chinese demands directly, there are straightforward ways for Chinese investors to overcome the obstacles easily and smoothly in the vast majority of cases.
CHINESE PERCEPTIONS AND COMPLAINTS

China complains that the regulatory process surrounding foreign acquisition of US companies is opaque, unreliable, highly politicized, and discriminatory against Chinese firms, with allegations that national security is used as a guise to block controversial takeovers. Is this an accurate appraisal?

Looking at the past, the Chinese complaints are not without reason. China first experienced the politics in Washington surrounding a foreign acquisition in 2005, when CNOOC, a 70 percent government-owned national oil company, proposed to buy the US oil company Unocal (Moran 2009; Moran and Oldenski 2013; Bergsten, Hufbauer, and Miner 2014).

Unocal produced 150,000 barrels of oil per day, of which 70,000 came from wells in the United States and 80,000 from wells in Asia. The principal concern was that Unocal’s oil production was a crucial commodity, too sensitive to fall into Chinese hands; a subtext of this concern was that US oil production would be diverted to China (in the worst case, sold directly to the People’s Liberation Army [PLA]). But 80,000 barrels of Unocal’s daily production were already sold into the highly competitive Asian market where alternative sources were easily fungible. The 70,000 barrels from US sources represented three-tenths of 1 percent of US daily consumption, with many alternative sources available to US buyers, and a potential diversion by CNOOC to China from the Gulf of Mexico would make Unocal wells the most expensive source of oil available to Chinese buyers, including the PLA. Unocal had no proprietary oilfield technology that was not available from multiple sources such as Halliburton and Schlumberger in international markets.

CNOOC submitted its proposal to CFIUS, which declined to begin assessment until the proposal had been presented to and accepted by Unocal’s shareholders. Meanwhile, the Washington Post reported that “members of Congress, many of them heavily lobbied by Chevron, lined up to attack CNOOC’s bid.” Chevron had already made its own lower-price offer to acquire Unocal. A nonbinding resolution in the House passed 398 to 15 appearing to preempt CFIUS, by asking the president to begin a special White House investigation of the acquisition. More authoritatively, Congress attached an amendment to the Energy Policy Act of 2005 (H6) instructing the administration to conduct a detailed examination of the impact of China’s growing energy needs on US national security, only after which CFIUS could begin its review.

Just eight days before Unocal shareholders were to vote on the CNOOC offer, the Chinese company withdrew its offer, citing “unprecedented political opposition,” and “a level of uncertainty that presented an unacceptable level of risk.” The battle was ceded to Chevron, which promptly proceeded with its own takeover of Unocal.

The CNOOC-Unocal case was soon followed by Dubai Ports World (DP World), showing that the politicized and erratic reaction in Washington to foreign acquisitions was not confined to China.

DP World sought to acquire the Peninsular and Oriental Steam Navigation Company (P&O), a British firm (Moran 2009, Moran and Oldenski 2013). P&O’s main assets were terminal facilities owned or leased in various ports around the world, including facilities at six US ports—Baltimore, Houston, Miami, New Orleans, Newark, and Philadelphia. CFIUS reviewed and approved the transaction, subject to the mitigation discussed below.

The proposed transaction first attracted broad public attention when a company named Eller, which was engaged in commercial litigation with P&O in London, contacted several Congressmen. The widely expressed fear was that the new parent company (in crude post-9/11 public opinion, an “Arab” parent company) might be lax in allowing dangerous persons or cargo into US port facilities that would be managed from headquarters in Dubai. A bipartisan group of ten senators, led by Charles Schumer of New York, signed a letter to the Senate leadership insisting that Congress be allowed to review CFIUS’s appraisal of the transaction and vote to approve or disapprove the CFIUS decision. The House Appropriations Committee passed a resolution of disapproval 62 to 4.

In point of fact, the six American ports to be acquired by DP World would be subject to the same container inspection and immigration regulations as any other US port. On top of this, however, CFIUS had taken the extra precaution of having the Department of Homeland Security (DHS) negotiate a “letter of assurances” with DP World, stipulating that the company operate all US facilities with management by US nationals, designate a corporate officer of American citizenship having the Department of Homeland Security (DHS) negotiate a “letter of assurances” with DP World, stipulating that the company operate all US facilities with management by US nationals, designate a corporate officer of American citizenship vetted by the Federal Bureau of Investigation (FBI) to serve as point of contact with DHS on all security matters, to promptly provide any and all information DHS might request, and assist other US law enforcement agencies on any matters related to port security. So the US ports managed by DP World would be the most carefully inspected ports in America.

Despite CFIUS approval, the political opposition to the proposed takeover was so vociferous that DP World announced that it would sell off the US port facilities acquired from P&O to a US company.

Little wonder therefore that Chinese commentators complain about unpredictability and discrimination in the treatment of proposed acquisitions in Washington. Among the reactions are:

The U.S. has the cold war mentality towards China and applies trade protection against Chinese companies. America prohibits China’s entry to many fields mostly due to political reasons. It abuses “national security” as an excuse.

—Bai Ming, Chinese Academy of International Trade and Economic Cooperation, February 2013

CFIUS is powerful because “national security” can be a block to many things. Why is “national security” a useful tool in the U.S.? Many Americans consider China as a potential competitor. The label of “threat to national security” has no cost and political gains. For example, using “national security” against a Chinese company in a campaign helps to win votes and support.

—Jia Xiudong, China Institute of International Studies, July 2014

CFIUS, a mysterious committee that keeps confidential its investigation process, objection reason and legal explanation, has been considered a roadblock in overseas investment in the U.S. by many Chinese companies, and even denounced as a tool for trade protection.

—Caixin, January 2014

But the CFIUS process has changed, largely in response to these two cases, with the FINSA regulations of 2009. In FINSA Congress wanted to strengthen the regulatory oversight of CFIUS. At the same time, the George W. Bush administration, spearheaded by Treasury Secretary Henry Paulson, wanted to regularize the appraisal of foreign acquisitions and ensure that CFIUS procedures to address national security threats coincided with the fundamental open door of the United States to foreign investment, a goal subsequently endorsed with White House and cabinet-level declarations by the Obama administration as well. The FINSA reforms attempted to mesh these two objectives.

**POST-FINSA CFIUS: PROCEDURES AND CASES**

FINSA strengthened the CFIUS process in several tangible ways: (1) while leaving the definition of “national security” open-ended, it expressly identifies transactions involving critical infrastructure (including energy assets) and critical technologies as deserving special scrutiny; (2) it requires more thorough investigation of all transactions involving state-owned enterprises (SOEs) or entities otherwise controlled by foreign governments; (3) it empowers CFIUS with the authority to negotiate, impose, and enforce mitigation agreements to address national security concerns; (4) it eliminates the safe harbor that had protected transactions cleared by CFIUS from future scrutiny (and potential unwinding), if parties to the transaction intentionally and materially breach any term of a mitigation agreement; (5) it introduces the US intelligence community, through the director of national intelligence, as a nonvoting member of CFIUS and requires an intelligence assessment for all CFIUS cases; and (6) it maintains the confidentiality of information provided to CFIUS as well as CFIUS deliberations and determinations.

Finally—and perhaps most importantly—FINSA formalizes CFIUS’s consultations with Congress, while providing a measure of insulation from politics. It requires CFIUS to provide written notice to Congress at the conclusion of both 30-day initial reviews and more extensive 45-day investigations, as well as detailed annual reports on its activities.

So post-FINSA CFIUS emerged stronger and more powerful than before. Has the treatment of foreign acquisitions in fact become less uncertain and more predictable in the ever-volatile politics of Washington? A look at two particularly controversial post-FINSA cases suggests that the answer might be affirmative.

The Congressional Research Service (Jackson 2014) identifies the acquisition of the US batterymaker A123 Systems and the takeover of US Smithfield Foods, both happening to involve Chinese investors, as the two post-FINSA cases arousing most congressional scrutiny and concern.

In December 2012 the Chinese auto parts manufacturer Wanxiang Group proposed to acquire the bankrupt electric car lithium-ion batterymaker A123. Prior to the acquisition A123 spun off its operations that supplied the US military to a US buyer. Members of Congress nonetheless argued that the acquisition would jeopardize US energy security. There were, however, more than a dozen alternative producers of lithium-ion batteries in the United States, Europe, and Japan. Others on Capitol Hill opposed the deal because A123 had been awarded nearly $250 million in federal grants to support clean energy technology, although Wanxiang had simply outbid other potential US buyers who sought the same assets. Despite these noises from Congress, CFIUS promptly approved the acquisition in January 2013 with no refilings, no mitigations, and no special security arrangements.

Even more controversial was the high-profile acquisition of Smithfield Foods by Chinese meat packer Shuanghui International Holdings in May 2013. Notwithstanding America’s historical role as a large exporter of agricultural products, Senator Debbie Stabenow (D-MI) termed the expansion of pork exports to China via the Smithfield acquisition a threat to what she labeled “food security.” She demanded that the secretary of agriculture be made a member of CFIUS. The Senate Agriculture
Committee called a special hearing on the acquisition, at which Smithfield’s CEO Larry Pope testified that the purpose of the acquisition of his firm was to help Shuanghui upgrade its food safety practices in China, while exporting more pork products to China (thus helping the US balance of payments). Some in Congress continued to express concern that somehow the acquisition would allow tainted pork products from China into the United States.

Despite all this activity on the Hill, CFIUS also approved the Smithfield acquisition smoothly, again with no refilings, no mitigations, and no special security arrangements.

So, while these are only two, albeit particularly controversial, cases, they are not offset by any CFIUS rejections of Chinese proposed acquisitions or any high-profile withdrawals of Chinese proposed acquisitions until the Ralls case—centered on a US court challenge, not congressional interference in post-FINSA CFU SI procedures—considered in the next section.2

It is impossible to dampen or control congressional behavior, so it may look to outsiders like nothing has changed in Washington. But post-FINSA, the CFIUS process of 30-day assessments for nontroublesome cases and 45-day investigations for more problematic cases (including all acquisitions involving foreign government-controlled companies from any country) has not been interrupted by congressional pressures, nor have congressional hearings or amendments imperiled the supremacy of CFIUS as the US government arbiter of potential national security threats via acquisition of US firms.

CHINESE FDI IN THE UNITED STATES AND CFIUS: LOOKING TO THE FUTURE

What is reasonable to predict about the flows of Chinese FDI into the United States in the coming years, and how will Chinese companies that invest via acquiring US companies be treated?

Chinese investment in the United States has been growing rapidly from a very low base (Hufbauer, Miner, and Moran 2015). More than half of the total stock of Chinese FDI entered in the past two years, amounting to $14 billion in calendar year 2013 and $12 billion in calendar year 2014. From 2007 to 2009, Chinese firms filed 13 notices with CFIUS, but from 2010 through 2012, they filed 39 notices, accounting for 25 percent of all notices. This includes 23 notices filed in 2012 alone, twice the level in the previous year (figure 1).3 In 2013 21 additional Chinese notices were filed with CFIUS. Of the 54 Chinese notices filed with CFIUS in 2011–13, 24 were in the manufacturing sector, 17 in mining, utilities, and construction, while the other 13 were in finance, information technology, and services.

From a comparative perspective, Chinese firms accounted for the largest number of filings in the three-year period 2011–13 (54 notices), followed closely by the United Kingdom (49 notices), Canada and Japan (34 notices each), and France (29 notices).

To predict future FDI flows, it is useful to deploy a gravity model for Chinese FDI much like gravity models that are used to estimate trade flows between countries based on variables such as per capita income, distance, and language (Moran and Oldenski 2013). Such a model shows clearly that despite the recent expansion of Chinese FDI, China’s investment level remains no more than half what would be expected on the basis of other such characteristics of the two countries. The gravity model predicts large and steady increases of Chinese FDI in the United States.

Using a less sophisticated predictive model based on (1) market size (total GDP measured at purchasing power parity [PPP] and population); (2) natural resources (natural resource rents as a share of GDP); and (3) governance, David Dollar (2015) also shows that China is underinvested in the United States and concludes that flows from China can be expected to rise rapidly in coming years.

What impact will these new and greater investment flows from China have on the US economy? Evidence from the Chinese FDI that has already taken place reveals that Chinese investors provide jobs with wages and benefits substantially higher than the average within the industries where they are located, on a par with the (higher) wages paid by US affiliates of firms headquartered in developed countries (Moran and Oldenski 2013). This is not surprising because the data show that Chinese companies come to the United States to perform R&D and gain management expertise as well as to sell goods and services to US consumers. So future flows of Chinese FDI are likely to provide good jobs to American workers.

Moreover, when foreigners invest in the United States their presence provides productivity spillovers to other firms in the sectors where they invest. These spillovers are not small: About 12 percent of the total productivity growth in the United States from 1987 to 2007 can be attributed to productivity spillovers from inward FDI (Moran and Oldenski 2013). Will the same be true for Chinese investors in the United States? Somewhat

2. As a member of Huawei’s International Advisory Council, it is not appropriate for the author to comment on the oddly sequenced SoftBank acquisition of Sprint in 2013 in which the parties preemptively pledged to Congressman Mike Rogers, chairman of the House Intelligence Committee, that they would not use Huawei equipment, a pledge that was subsequently affirmed in the approvals granted by CFIUS and the Federal Communications Commission.

surprisingly, foreign investment on the part of companies from developing countries—including China—already also generate statistically significant productivity spillovers (the data do not permit the isolation of productivity gains supplied by Chinese investors specifically, but they do show that Chinese investors conduct much higher levels of R&D in the United States than other investors from the developing world). These spillovers are likely to continue and grow in magnitude.

Around the globe, some 80 percent of all FDI takes place via foreign companies taking over local firms, depending on the industry. In the case of Chinese investments in the United States—37 percent of all investments by number of transactions and 84 percent of all investments by size of transaction—have taken place via acquisition between 2000 and mid-2015.4 So it is reasonable to expect that a large proportion of Chinese investment will continue to involve acquisitions of US companies.

How will CFIUS receive future acquisitions? In particular, will Chinese investors achieve the nondiscriminatory and reasonably transparent treatment that they desire? Certainly not in any formal or legal way, but Chinese objectives can largely be achieved nonetheless as a practical matter in the vast majority of cases.

**Chinese Demands for Formal or Legal Nondiscriminatory and Transparent Treatment Will Not Be Met**

The purpose of CFIUS is to protect the United States against national security threats that might emerge from foreign takeovers of US firms.

CFIUS leadership and US government spokespersons more generally assert that they scrutinize foreign investment in a nondiscriminatory fashion. To quote Assistant Secretary of Treasury Marisa Lago, head of CFIUS investigations, “Third—and I want to emphasize this point—CFIUS does not discriminate among the countries of companies seeking to invest in the United States….”5 That is surely an inaccurate use of words—CFIUS representatives may mean that CFIUS scrutiny of Chinese acquisitions is careful, objective, and follows the same procedures as for acquisitions by firms from other countries, but CFIUS scrutiny of Chinese acquisitions is certainly not nondiscriminatory, if the intent of the term nondiscriminatory is offering Chinese investors anything approaching most favored nation (MFN) treatment.

In a world characterized by geopolitical tensions between major powers it is simply naïve to think that acquisitions by companies from China, Russia, and other potential US adversaries would not receive more thorough and intense scrutiny than acquisitions by firms from close allies. This more-intense scrutiny will be particularly true for SOEs from China, Russia, and other potential adversaries.

Moreover, in terms of the day-to-day workings of CFIUS, while the staff and political-appointed leadership from Treasury, US Trade Representative, and some other agencies can be expected to be generally pro-FDI, the staff and political-appointed leadership from the Department of Defense, DHS, and Department of Justice/FBI can be expected to be worst-case-scenario experts toward foreign acquisitions. Staff members from these latter agencies are trained, selected, evaluated, and motivated to provide investigations of differential intensity.

---


Finally, FINSA requires the nonvoting intelligence agencies to complete a “capability” and “intent” assessment of transactions, and the “intent” assessment draws on National Security Agency (NSA) and Central Intelligence Agency (CIA) capabilities that are specifically targeted at potential adversaries like Russia and China. This fact will be important in preventing public revelation of what suspicions might dominate CFIUS assessments, which is treated next.

With regard to transparency, CFIUS is required by law to keep its assessments confidential for business and commercial reasons. This legal mandate is reinforced by the determination of the US intelligence agencies to keep their assessments secret so as not to reveal “sources and methods” used in their investigations.

To what extent might the path-breaking Ralls case change the transparency of CFIUS assessments?

In March 2012, without reporting the transaction to CFIUS, Ralls Corporation, a Chinese-owned firm, acquired several wind farm projects whose towers overlooked restricted Naval Weapons Systems Training Facility airspace, where the newest generations of drones (unmanned aerial vehicles) are tested. In June, CFIUS contacted Ralls and requested that the firm file a voluntary notification to have its investment retroactively reviewed. After giving the acquisition a preliminary examination, CFIUS asked that Ralls stop operations until a complete investigation could be completed. Based on that investigation, including confidential US Navy inputs, CFIUS recommended that President Obama block the investment by ordering a divestment of the transaction as well as removal of equipment already installed, which he did through an executive order on September 28, 2012. This was only the second such formal US prevention of a foreign acquisition.

In response, Ralls filed a suit in the US District Court for the District of Columbia arguing that the company was treated unfairly under the Due Process Clause of the Fifth Amendment to the US Constitution because the CFIUS review process did not offer the company an opportunity to review, respond to, and rebut any evidence used to make a presidential determination. CFIUS has never offered the parties a chance to review, respond, and rebut allegations made against them. The district court ruled that it lacked jurisdiction on this motion but indicated that it would not prohibit Ralls’s due process claim from proceeding. On July 15, 2014 a three-judge panel of the US Court of Appeals for the District of Columbia ruled that the CFIUS decision violated Ralls’s due process rights and that CFIUS must therefore explain before the DC district court why it blocked the company’s wind farm construction and give the company a chance to rebut. But the court acknowledged that the government has a national security interest in withholding classified information and is obliged to reveal only unclassified information used to oppose the transaction. The appeals court remanded the case back to the DC district court, where the case sits today.

So, even if upheld, the Ralls ruling is likely to provide only limited comfort to companies that want to know what allegations are being held against them and to have a fair opportunity to rebut such charges, to the extent some such allegations are based on confidential or secret information.

In light of this preceding analysis, how might Chinese objectives for more predictable and transparent treatment be met?

How Might Potential Chinese Investors Gain Greater Predictability?

Despite the deliberately open-ended definition of national security threats in CFIUS regulatory instructions, the threats to national security that CFIUS has identified over the past four decades can be separated into three distinct types, and the conditions under which each threat becomes plausible can be distinguished from situations in which the harm envisioned is not credible (Moran 2009, Moran and Oldenski 2013). This threat-assessment tool is drawn from investigation of the universe of CFIUS cases; it does not represent specific legal guidance to CFIUS.

The first threat springs from the ability of the foreign acquirer, acting independently or under instructions from the home government, to delay, deny, or place conditions upon provision of output from the newly acquired producer. To assess the plausibility of this threat of manipulation of access requires a two-step analytic process. The first step is a calculation of how “crucial” or “critical” the process or product is—crucial or critical is defined as the cost of delay or doing without. The second step is a calculation of how concentrated the international industry is, how abundant are near-substitutes to the process or product of the company that is being acquired, and how high are switching costs. If the goods and services of the company being acquired are widely available and switching costs are low, there is no plausible threat to US national security.

The second threat derives from a possible leakage of sensitive technology to a foreign company or government that might deploy or sell such technology so as to harm US national interests. To assess the plausibility of Threat II is once again a two-step process. Step one is to calculate the damage that could be done if the technology were deployed against US interests. Step two is to calculate how readily available such technology is in international markets to see if it made sense to refuse the transfer to foreign hands. If alternative sources of the technology held by the acquired firm are widespread, national security will not be served by blocking the transaction.
The third threat derives from the potential that acquisition of a US company might allow a foreign company or its government to penetrate the US company’s systems so as to watch over, monitor, or place time-bombs within those systems. If alternative suppliers of the goods and services from the company to be acquired are readily available, any user who feared penetration could simply switch to another provider. As discussed later, however, figuring out how to cope with this threat in a world of globalized supply chains—especially in the information technology (IT) sector—creates difficult quandaries for CFIUS.

[The three threats] decision tree should reassure Chinese investors...that the vast majority of cases will pose no credible national security threat whatsoever.

Would-be Chinese investors can use the decision tree shown in figure 2—which is derived from the three-threat assessment of the entire corpus of previous CFIUS cases—to predict how CFIUS is likely to assess their specific proposed acquisition. The use of this decision tree should reassure Chinese investors—like all foreign investors—that the vast majority of cases will pose no credible national security threat whatsoever.

Only if the US firm to be acquired controls access to a critical good or service that does not have substitutes in the international market, or if the US firm to be acquired gives over a sensitive semi-unique technology that could be deployed at great cost against US interests, or if the target US firm could be used for penetration or surveillance in ways damaging to the United States without the ability of US users to switch to other more secure alternatives will a credible threat to US national security exist.

Investments by SOEs or other firms where there is evidence of foreign government control will undergo a mandatory second 45-day investigation, after the initial 30-day scrutiny (27 percent of Chinese acquisitions involved SOEs during 2000–15), but acquisitions by SOEs will not be blocked unless they pose one of the three threats above.

The use of this decision tree is the closest would-be foreign investors—from any country—can come to predicting the treatment they will receive from CFIUS when they choose to invest via acquisition.

How Might Potential Chinese Investors Gain Greater Transparency?

In those sensitive cases where an acquisition might pose a plausible national security threat, how can potential Chinese investors gain greater transparency about CFIUS allegations or suspicions, especially if those acquisitions are based on confidential or secret information?

Here is where the ongoing confidentiality of CFIUS assessments and secrecy of intelligence agency appraisals always pose problems. First-time Chinese SOEs and private Chinese firms that are wary of Washington can follow the path that more experienced Chinese investors—as well as Arab, Russian, Israeli, and French investors—have become accustomed to taking to move forward on acquisitions when they do not know exactly what is holding up CFIUS approval. They seek expert counsel.

The lawyers from the top dozen or so law firms that deal with CFIUS cases—many of whom are former CFIUS staff members—are accustomed to playing a form of twenty-questions with current CFIUS officials. In the face of CFIUS objections and requests for more information, they ask: Might the divestiture of this division be helpful in moving this CFIUS decision forward? Might the establishment of an all-American board to supervise these particular operations speed up the CFIUS deliberations? Might a commitment to keep data on American soil subject to subpoena by a US court satisfy CFIUS concerns? And so on.

At the end of the day, these techniques employed by experienced practitioners on behalf of the acquiring firm are the closest that investors from China, Russia, Arab countries, or other states with controversial geopolitical objectives come to achieving a degree of transparency when they propose to invest in the United States via acquisition.

Some cases—such as acquisition of high-tower facilities overlooking restricted US military sites by Chinese or Russian companies, or by Lebanese or Cypriot firms (which not infrequently are front companies for problematic owners), or by companies of a handful of other national origins—might simply not be mitigable.

Special Concerns about Foreign Acquisitions in the IT Sector in an Era of Globalized Supply Chains

Threat III assessments—involving penetration, surveillance, even placing time-bombs in the goods and services of the acquired firm—pose a conundrum for CFIUS in the contemporary era of globalized IT supply chains.

---

All the basic building blocks of IT systems—including servers, routers, data storage and retrieval mechanisms, flash drives, and microchips—have hardware and software components that derive from production sites in China, Taiwan, Russia, Israel, Eastern Europe, Malaysia, the Philippines, and Mexico, all of which are susceptible to surreptitious engineering inputs.

To be sure, software inputs from Manila and Guadalajara might seem more secure than from Beijing and Moscow, but to worse-case skeptics on the CFIUS team mere geography alone may not provide adequate comfort.

It is an illusion to think that Threat III penetrations can be eliminated by singling out and discriminating against providers on the basis of the parent company’s national origin, such as rejecting Chinese-owned providers while allowing purchases of hardware and software from US or, say, French (Lucent-Alcatel) or Swedish firms (Ericsson) whose assembly facilities are adjacent to the Chinese-owned plants in Shenzhen (Moran 2013).

CFIUS showed the simplistic approach to protecting national security when Bain Capital proposed in late 2007 to acquire 3-Com, with a 16.5 percent minority shareholding by Huawei. As always, CFIUS appraisals are not made public but it was widely assumed that the participation of a Chinese company in the acquisition might open potential Threat III penetrations by the Chinese. Amidst great controversy—but without a formal CFIUS ruling—Bain withdrew its offer to acquire 3-Com in March 2008.

More recently, CFIUS had to face the conundrum of globalized supply chains head on when the Chinese firm

### Figure 2  Decision tree to assess national security rationale for blocking foreign acquisition

- **Criticality test**
  - Threat I: How much would the costs be if the acquired firm's goods or services were denied or conditions placed upon their supply?
  - Threat II: How much national security-related advantage would be gained by the foreign purchaser and its government if the foreigner gained control of the target firm?
  - Threat III: How extensive would the damage be from surveillance or disruption through foreign ownership of a given network?

- **Plausible threat test**
  - Are there widely available substitutes for goods and services of target acquired firm in global markets, competitive suppliers in global markets, low switching costs?

- **High criticality**
  - High plausibility
  - Block foreign acquisition: Only if it leaves the nationally owned target of acquisition internationally competitive or capable of being internationally competitive

- **Low plausibility**
  - Allow foreign acquisition

- **Low criticality**
  - Allow foreign acquisition

Source: Moran and Oldenski (2013).
Lenovo proposed to acquire IBM’s X86 server business in 2014. The IBM low-end X86 server had been widely used by businesses, government agencies (including defense and intelligence agencies), and principal IT trunk carriers like ATT and Verizon. The Threat III concern again was that these commonplace X86 servers might become a vehicle for some kind of penetration by Chinese agencies. But most X86s were already produced in China, by Hewlett-Packard and Dell, for example, as well as by IBM, using thousands of Chinese engineers and tens of thousands of Chinese inputs. Since CFIUS approved this acquisition, it must have concluded (recalling, again, that how CFIUS makes its determinations is not released to the parties or to the public) that the marginal increase in threat from Lenovo ownership was insignificant.

How might it be possible to deal realistically with ensuring supply chain integrity when hardware and software, plus patches and upgrades, come from thousands of sources around the world?

One method would be to establish government-run cybersecurity evaluation centers around the world to which IT companies entrust their source code. Experts at these centers could vet goods and services on offer from IT companies through large random samples, which receive an embedded time/date stamp upon inspection that a subsequent user can verify to ensure that no changes were made to the code after it left the evaluation center.

The UK National Security Adviser has recommended and implemented this model to deal with Huawei products sold in the United Kingdom (Cabinet Office and National Security and Intelligence 2015). The chairman of the board of the Cyber Security Evaluation Center at Banbury is the director general for cybersecurity at GCHQ, the British equivalent of the US NSA. Similar cybersecurity centers in North America, Europe, and Asia—and indeed in China and Russia—set up to examine IT inputs from all sources on a random basis would not be able to monitor every single IT product sold anywhere, but these evaluation stations could go a long way toward providing reassurance about global supply chain integrity.

CONCLUSION

The analysis in this Policy Brief supports the assessment that large new amounts of Chinese FDI will surely flow into the United States. Within these rising flows, Chinese acquisitions that might pose genuine national security threats can be carefully separated from those that do not. Such rigorous assessment will show that very few inward acquisitions will pose any threat whatsoever. The overwhelming bulk of Chinese investments should be welcomed without hesitation. They will benefit US workers, firms, communities, and consumers.

REFERENCES


This publication has been subjected to a prepublication peer review intended to ensure analytical quality. The views expressed are those of the author. This publication is part of the overall program of the Peterson Institute for International Economics, as endorsed by its Board of Directors, but it does not necessarily reflect the views of individual members of the Board or of the Institute’s staff or management.

The Peterson Institute for International Economics is a private nonpartisan, nonprofit institution for rigorous, intellectually open, and indepth study and discussion of international economic policy. Its purpose is to identify and analyze important issues to make globalization beneficial and sustainable for the people of the United States and the world, and then to develop and communicate practical new approaches for dealing with them. Its work is funded by a highly diverse group of philanthropic foundations, private corporations, and interested individuals, as well as income on its capital fund. About 35 percent of the Institute’s resources in its latest fiscal year were provided by contributors from outside the United States. A list of all financial supporters for the preceding four years is posted at http://piie.com/supporters.cfm.