

Foreign Direct Investment: National Security and the Role of CFIUS

**by
Maeve Dion**

First published in the Journal of Homeland Security (March 2009).

Introduction

The risk of foreign access to, or control of, important domestic assets is considered a national security threat in many countries, including the United States. The United States uses various mechanisms to mitigate such threats. Foreign ownership is prohibited in certain industries, such as nuclear power generation. In some regulated industries, the government may compel foreign owners to comply with additional security provisions in order to receive operating licenses. The government also may include security provisions in its procurement contracts with foreign suppliers and service providers. Perhaps the most far-reaching mechanism for mitigating these kinds of national security threats is the Executive Branch's jurisdiction over foreign direct investment.

The United States has a review process for all foreign direct investment that may present national security risks due to foreign access to, or control of, critical domestic assets and resources. The Committee on Foreign Investment in the United States (CFIUS) has existed for more than 30 years and is mandated by a Federal statute that was most recently amended in 2007.

History of CFIUS

In the 1970s, Congress became concerned with increasing Arab direct investment in the United States; lawmakers feared that members of the Organization of Petroleum Exporting Countries, who were then profiting from increasing oil prices, would invest in strategic US assets.¹ President Ford issued an Executive Order in 1975 to create the Committee on Foreign Investment in the United States.² Under this authority, the inter-agency CFIUS acted as a general investigator and policy advisor; specifically, CFIUS was responsible for “monitoring the impact of foreign investment in the United States, both direct and portfolio, and for coordinating the implementation of United States policy on such investment.”³ For its first decade, CFIUS had no strong screening power and acted completely at the discretion of the President.⁴

In the 1980s, however, Congress again became concerned with FDI, this time in parallel with the increasing trade deficit. Foreign investment had been expanding,⁵ and Congress was particularly focused on Japanese and Chinese acquisitions⁶ and the potential for foreign economic espionage toward the US technology industry, which was at that time more advanced than in most other countries.⁷ One particularly contentious transaction was Fujitsu's attempted purchase of 80% of Fairchild, a U.S. semiconductor manufacturer. Arguments against the transaction included claims that the United States would become dependent upon Japan for semiconductors; that the transaction would impair U.S. competitiveness; and that Japan would gain access to critical US technologies. With Congress demanding some sort of action, President Reagan agreed to institute a national security assessment of Fujitsu's offer. Since CFIUS merely had powers of review, with no authority to restrict or block the transaction, President Reagan had to order the review under U.S. antitrust laws. However, due to political debate and pressure, Fujitsu withdrew its offer for Fairchild.⁸

As a result of the Fujitsu-Fairchild offer, and other similarly controversial acquisitions and attempts, Congress determined that the United States needed a stronger mechanism for reviewing FDI — something that had the power to prevent sensitive transactions.⁹ Congress also wanted to encourage the President to more vigorously investigate foreign investments that had the potential to damage U.S. national interests.¹⁰ The resulting proposal was the Exon-Florio¹¹ amendment to Section 721 of the Defense Production Act, passed as part of the Omnibus Trade and Competitiveness Act of 1988.¹² The amended Section 721 authorized the President or his designee (1) to investigate direct foreign investments that might pose national security risks and (2) to suspend or prohibit the transaction or to order divestiture for a completed sale.¹³ In January of 1989, President Reagan issued Executive Order 12661 that amended President Ford's Executive Order and named CFIUS as the President's designee under Section 721.¹⁴

Several years later the CFIUS-empowering authorities were again amended, and again the amendments came in the wake of another controversial, attempted acquisition of a technology company. This time the target was a leading defense company with expertise in missile technology; the foreign acquirer was French, and the government of France owned a majority interest in the company, including a majority of the voting stock.¹⁵ Although the acquisition was not accomplished, Congress was motivated to amend Section 721 to reflect the concern that a foreign acquirer could be acting on behalf of (or could potentially be controlled by) a foreign government.¹⁶ The legislative changes, designated the "Byrd Amendment," (1) required a longer period of investigation for such transactions and (2) attempted to enhance congressional oversight and transparency by ordering quadrennial Critical Technologies Reports to track foreign economic espionage and foreign governments' investment strategies in the U.S. critical technology industry.¹⁷

The crux of the CFIUS requirements, and the basis for other restrictions on foreign direct investment — restrictions (such as licensing procedures and procurement rules) based on national security — is the concern that a foreign owner may not have as strong an interest in U.S. national security as a domestic owner. While such concerns may be ameliorated via contractual security provisions and proxies or other voting mechanisms for the majority of foreign direct

investment that is motivated purely by financial returns, there may still exist the *potential* of strategic control by a foreign government — that is, if strategic interests of the foreign government supersede fears of contractual liabilities, the security agreements may be breached and national security may be imperiled.

For 15 years after the Byrd Amendment, the CFIUS process continued without any substantial changes (with merely a few revisions to the membership of CFIUS). If a proposed foreign direct investment transaction posed a national security threat, one of three things usually happened: (1) the foreign acquirer restricted its ownership structure so that “control” was not implicated; (2) the foreign acquirer entered into security agreements (contracts) with the CFIUS member agency(ies) to mitigate the threat by restricting the foreign acquirer’s discretion in ownership structure, business operations, or personnel decisions; or (3) the parties withdrew their CFIUS notice and either canceled the transaction or delayed it to negotiate changes that would satisfy a later CFIUS review.¹⁸

In these intervening years, CFIUS operated with broad discretion in its security assessments and with strict confidentiality controls. While the statute itself did not change during the 15 years following the Byrd Amendment, CFIUS reviews evolved to incorporate the changing threat environment. For example, even before the terrorist attacks of September 11, 2001, CFIUS reviews of telecommunications transactions had become more stringent, in part due to the globalization of the communications industry and the increasing reliance on telecommunications in critical functions and services.¹⁹ Besides substantive changes due to evolving threats, over time CFIUS developed various internal processes to better fulfill its national security mandate. For example, the CFIUS member agencies developed informal procedures to encourage early communication between themselves and potential foreign investors, to identify and mitigate security concerns before the transaction was even filed officially with CFIUS.

However, CFIUS unfortunately did not excel in all of its duties. In one glaring example, although the Byrd Amendment had attempted to enhance oversight and transparency with certain reporting requirements, CFIUS did not properly fulfill these requirements, and Congress did not pressure CFIUS to comply. Rather than one report every four years, only two Critical Technologies Reports were ever made -- one in 1994 (a couple of years after the Byrd Amendment) and one dated 2006 but delivered to Congress in 2007. The [more recent report](#) was crafted in the midst of media and Congressional furor over perceived mismanagement of CFIUS.

In the early and mid-2000s, Congress became increasingly concerned about various perceived deficiencies in the CFIUS process, as highlighted by specific transactions which received much attention in the media (for example, Lenovo-IBM, CNOOC-Unocal, Dubai Ports World-P&O Steam Navigation Company). In response, Congress again amended Section 721, this time with the [Foreign Investment and National Security Act of 2007](#), which came into effect on October 24, 2007.

FINSA

FINSA significantly changed the text of the CFIUS statute, and the changes were heralded by much fanfare in the press. However, the new law did not significantly affect the crux of the CFIUS mandate; nor did it make sweeping changes to the internal process. Not all of the changes will be discussed in this article — for example, new requirements regarding certification by the parties to the transaction, CFIUS certifications to Congress at the end of each review, and non-delegation of certain authorities. Rather, this section reviews the basics of the CFIUS process and addresses some of the main issues that have garnered most of the attention in CFIUS debates.

*Basics of CFIUS*²⁰

As described in [Table One](#), CFIUS impacts any merger, transaction, or takeover, by or with any foreign entity, which could result in foreign control of an entity engaged in U.S. interstate commerce. Before formally filing any papers with CFIUS, parties to a transaction may talk with CFIUS member agencies to determine if their transaction is likely subject to a CFIUS review, and if so, what national security concerns are implicated and what measures could mitigate those concerns. Parties thus can (1) structure their transaction to better satisfy CFIUS demands, (2) have a more reliable expectation regarding the timeframe for concluding the transaction, and (3) better manage communication of the transaction with shareholders and press to lessen potential detrimental market perceptions and effects. This section of FINSA thus incorporated the already-existing informal practices of CFIUS.

CFIUS reviews may be initiated in a couple of ways. Any party to a relevant transaction (pending or already completed) may submit a written notice to CFIUS, identifying the transaction and providing the mandated information. Also, any CFIUS member agency or the President may (1) unilaterally initiate review of a relevant transaction, (2) unilaterally re-open review of a transaction that has already undergone CFIUS review if in the original CFIUS review any party submitted false or misleading material or omitted material information, or (3) re-open review of a transaction that has already undergone CFIUS review if the original CFIUS review resulted in a security agreement or other mitigation measure and a party intentionally materially breached the agreement or mitigation measure, if the breach is certified by the relevant CFIUS member agency, and if CFIUS determines that there are no other remedies or enforcement mechanisms to address the breach.

Within 30 days of receiving written notification, CFIUS must review the transaction to determine if it affects U.S. national security. The CFIUS member agencies consider factors specified by legislation and by CFIUS regulation, and other factors implicated by the specific transaction being reviewed (a case-by-case assessment). Statutory factors include:

- Domestic production capabilities and capacities required for national defense and national security.

- The potential effects of the foreign acquisition on (1) sales of military equipment or technology to certain countries of concern, (2) U.S. global leadership in national security-related technologies, (3) national security in relation to U.S. critical infrastructure and critical technologies, (4) potential transfer of dual-use technologies, and (5) long-term US requirements for energy and other critical resources.
- Whether the foreign acquisition is a foreign government-controlled transaction (as statutorily defined).
- Adherence of the foreign acquirer's country to nonproliferation controls.
- The relationship between the foreign acquirer's country and the United States, particularly regarding counterterrorism efforts.

CFIUS must further investigate the transaction (basically an extended review, to last no longer than 45 days from the start of the investigation) and must take necessary mitigation actions if at the end of the review period any one of the following three situations applies: (1) the lead CFIUS agency recommends and the other CFIUS member agencies concur, that an investigation is needed for further assessment of the transaction; (2) there still exists an unmitigated threat to national security; or (3) the transaction could result in the control of any entity engaged in US interstate commerce by a foreign government or entity controlled by or acting on behalf of a foreign government. However, for this third situation, involving foreign government control, there is an exception from the mandatory investigation: if CFIUS determines that the transaction will not impair US national security, then no investigation is required.²¹

If the review and/or investigation resulted in modifications to the transaction, and/or security agreements between the CFIUS member agency(ies) and the parties to the transaction, the designated lead CFIUS agency for the transaction is authorized to monitor and enforce the agreements.

At the conclusion of the investigation, if the transaction is determined to impair U.S. national security, the president may take appropriate action to suspend or prohibit the transaction. The president's determinations and actions are not reviewable in any court of law. The president may direct the U.S. attorney general to pursue relief, including divestment, in U.S. federal courts in order to implement and enforce this authority. However, the president may only exercise the authority under this paragraph if (1) based on credible evidence, the president believes that the controlling foreign entity might take action that threatens to impair U.S. national security and (b) other provisions of law (excluding the International Emergency Economic Powers Act) do not provide adequate and appropriate authority to protect U.S. national security in relation to the transaction.

Mandatory Investigations

Although the publicity surrounding FINSA focused on the new mandatory investigation period for transactions controlled by a foreign government and for transactions involving critical infrastructure, both of these mandates have exceptions, and these exceptions are so encompassing that they almost overwhelm the “mandate.” Basically, if it is determined that the transaction will not impair national security, then no investigation is required. Thus, if a transaction does not pose a risk to national security, then there is no requirement for an additional 45-day investigation, even if the transaction involves critical infrastructure or is a transaction controlled by a foreign government. Note that FINSA states that the risk determination may be made jointly by the CFIUS chair and the designated lead CFIUS agency for the transaction. However, CFIUS has historically acted by consensus, equally valuing the risk assessments of the various member agencies. Thus in January 2008, President Bush noted in Executive Order 13456 that CFIUS must initiate an investigation if any member agency deems the transaction to be an unmitigated risk to national security.²²

The distinction between the 30-day review and subsequent 45-day investigation periods may in reality be a distinction without a difference, for several reasons. First, many CFIUS reviews begin well before formal notification — parties to a pending transaction often communicate early with various CFIUS member agencies so that they can anticipate the likely national security requirements and build the mitigation factors into the transaction agreements. Thus the review may occur over a period of months, not just for 30 days. Second, in practice there may be little difference between the CFIUS activities in the “review” and “investigation” stages. The goal in both is to discover and mitigate potential risks to national security; the CFIUS member agencies use their own internal methods to accomplish this goal, and these methods do not vary just because the process has moved from the 30-day period to an additional 45 days.

Follow-Up & Enforcement

FINSA created new requirements for follow-up and enforcement of CFIUS mitigation agreements (and other CFIUS-required preconditions to the transaction) entered into by CFIUS member agencies and the parties to the transactions. In the past, each CFIUS member agency conducted follow-up and enforcement based upon the respective agency’s internal processes — there was no common procedure, and thus no common tracking mechanism or comprehensive congressional oversight. Under the new law, CFIUS must use common methods for evaluating compliance with the mitigation agreements. For each transaction, the lead CFIUS agency is required to monitor and enforce the agreement, and to report any future material modifications to all relevant federal agencies and departments.

Congressional Oversight

The amendments to the CFIUS law created new provisions that increase congressional oversight, including notifications of completed CFIUS reviews; certifications of completed investigations; briefings of specific transactions or mitigation agreements and conditions; detailed annual

reports of all reviews and investigations, including comprehensive assessments of possible trends in foreign investment; and annual reports of trends of foreign investment in critical technologies (note that this is a change from the previously-required *quadrennial* Critical Technologies Reports).

Membership

FINSA mandates that the CFIUS members include the Secretaries of Treasury, Homeland Security, Commerce, Defense, State, Energy, and Labor; the US Attorney General; the Director of National Intelligence; and the heads of other executive departments or offices that the president deems appropriate. These members may appoint designees to act on their behalf. By Executive Order in 2008, the president added two additional members: the U.S. Trade Representative and the Director of the Office of Science and Technology Policy. Further, the president noted that certain other representatives should observe and participate in CFIUS activities as appropriate: the Director of the Office of Management and Budget; the Chairman of the Council of Economic Advisers; and the Assistants to the President for National Security Affairs, Economic Policy, and Homeland Security and Counterterrorism.²³

National Security

The new law specifically states that “national security” includes issues of homeland security and related critical infrastructure concerns. “National security” in this context has not been explicitly defined in past legislation, and it was not further defined in the statute, leaving it up to CFIUS to apply the definition case by case, pursuant to the CFIUS regulations. The phrase “economic security” was not added, nor has it ever been a statutory factor. Forthcoming regulations should provide examples of transactions that have presented national security risks.

Practical threats implicated by the overarching concerns of national security in the CFIUS process have been compiled by Graham and Marchick, who identify the common, perceived threats as:

- Shutting down or sabotaging a critical facility in the United States.
- Impeding a U.S. law enforcement or national security investigation.
- Accessing sensitive data, or becoming aware of a federal investigation or methods used by U.S. intelligence and/or law enforcement agencies, including moving transaction data and records offshore.
- Limiting U.S. government access to information for surveillance or law enforcement purposes.
- Denying critical technology or key products to the U.S. government or U.S. industry;

- Moving critical technology or key products offshore that are important for national defense, intelligence operations, or homeland security;
- Unlawfully transferring technology abroad that is subject to U.S. export control laws;
- Undermining U.S. technological leadership in a sector with important defense, intelligence, or homeland security applications;
- Compromising the security of government and private-sector networks in the United States;
- Facilitating state or economic espionage through acquisition of a U.S. company; and
- Aiding the military or intelligence capabilities of a foreign country with interests adverse to those of the United States.²⁴

Critical Infrastructure

One of the recent changes enacted by FINSA was the incorporation of the phrase “critical infrastructure” into national security considerations. In CFIUS reviews, investigations, and determinations by the president, one of the factors enumerated by Congress is: “the potential national security-related effects on United States critical infrastructure, including major energy assets.”²⁵ Another section of the new law — specifying when investigations are mandatory rather than discretionary — addresses transactions that would result in control of any U.S. critical infrastructure by or on behalf of any foreign entity.²⁶

The new legislative attention to critical infrastructure was not a result of a failure to consider critical infrastructure in past CFIUS processes. In fact, prior to the 2007 amendment, numerous CFIUS reviews had been conducted for transactions in critical infrastructure industries such as telecommunications, energy, and aerospace. It therefore appears that the statutory addition of “critical infrastructure” to the CFIUS law really only has the effect of incorporating a general policy consensus that “national security” should include not only protection of the traditional military and defense industrial base, but also protection of other critical infrastructures.

In defining “critical infrastructure” in the context of CFIUS, Congress paraphrased from the standard Federal definition (first defined in the USA Patriot Act), finding that critical infrastructure included “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security.”²⁷ Congress stated that the definition of “critical infrastructure” is further subject to CFIUS regulations. The 2008 proposed regulations do not refine this definition; however, CFIUS is required to issue guidance on the kinds of transactions that implicate national security risks, including those transactions that could involve the risk of a foreign government’s control of U.S. critical infrastructure. With this guidance and perhaps with the increased congressional oversight and transparency, it may be possible to observe how the

term “critical infrastructure” is defined in application based upon the case-by-case CFIUS assessments of various transactions.

Conclusions

Events of the past 10 to 15 years have evolved an increasing perception of vulnerability to domestic attacks. In the current atmosphere, national security restrictions may not always be based on the likelihood of foreign attacks or infiltration of U.S. infrastructure, but on the fear of potential catastrophic consequences that may occur as a result of foreign attack, however unlikely. (Perhaps this partly explains the blanket prohibition on foreign ownership of nuclear power facilities.)

On the other hand, the national security analyses of CFIUS are historically based on risk assessments of each transaction, made one case at a time. In parallel with this risk management approach, however, there may be political pressure from public and congressional unease with the mere concept of foreign ownership of sensitive U.S. assets. Such pressure is only worsened by an opaque CFIUS process that neither publicly discusses its level of confidence in the lack of national security threat by a specific foreign acquirer nor explains any negotiated mitigation measures. While much of this detailed information must properly be kept confidential, and proprietary business information must not be disclosed, surely there is a better way for CFIUS to communicate with both congress and the American public regarding its confidence in the security of foreign direct investment in the United States.

With the new FINSA transparency requirements, CFIUS should capitalize on the opportunity to present timely analyses and reports on its activities. While details of specific transactions may be protected, the annual reports should include an unclassified assessment of that year’s CFIUS activity, so that the public may understand how CFIUS vigorously protects national security while still ensuring that the United States accrues all of the many benefits of foreign investment.

Besides general reporting responsibilities, CFIUS must provide more detailed information to businesses that may be subject to CFIUS reviews. As computer and information infrastructure (as well as other critical infrastructure) increasingly become more important to U.S. national security, the number of foreign acquisitions potentially subject to CFIUS may increase accordingly. Further, in the last few decades, numerous industries have shifted to globalized business and economic structures, thereby increasing foreign trade and investment opportunities. With the broad application of “national security” in the CFIUS context, and with the CFIUS process of case-by-case review, it is difficult to determine, *ex ante*, whether a specific transaction is likely to implicate CFIUS concerns. This lack of clarity is frustrating to businesses that rely on dependable factors in their decision making, especially in relation to mergers and acquisitions. As mentioned above, some of the new changes enacted with FINSA require that CFIUS begin to provide guidance on the kinds of transactions that could pose national security concerns; this guidance will help businesses better predict CFIUS concerns in potential foreign acquisitions.

Since the writing of this article in August 2008, the [final revised regulations](#) and [new agency guidance](#) were issued. The final rule was published at 73 Fed. Reg. 70702 and became effective on December 22, 2008. The Guidance Concerning the National Security Review Conducted by CFIUS was published at 73 Fed. Reg. 74567 (Dec. 8, 2008). As discussed in this article, the guidance provides information on the CFIUS process, focusing on how CFIUS analyzes the national security considerations within a proposed transaction.

With the enactment of FINSA, Congress enhanced its oversight role in CFIUS. In the past, however, Congress was not diligent in enforcing CFIUS compliance with the single reporting requirement of the Critical Technologies Reports. Rather than waiting for the next contentious transaction to hit the media and inflame the public, Congress should be proactive in its new expanded oversight, demanding timely reporting, notifications, and briefings. The CFIUS process is meant to protect the United States from various national security risks related to foreign access to, or control of, important domestic assets. Better transparency and reporting requirements will help to publicly demonstrate the validity of this premise — or will help to identify further refinements to a policy that strives to balance national security restrictions with encouragement of foreign investment and the demands of globalization.

TABLE ONE

The Committee on Foreign Investment in the United States (CFIUS)

THE PROCESS OF NATIONAL SECURITY REVIEWS AND INVESTIGATIONS
OF FDI-IMPACTED MERGERS, ACQUISITIONS, OR TAKEOVERS

I. Relevant Transactions

- Any merger, transaction, or takeover;
- AND • proposed or pending after August 23, 1988;
- AND • by or with any foreign entity;
- AND • which could result in foreign control of any entity engaged in US interstate commerce.

II. Preliminary Activity

Parties to a transaction may talk with CFIUS member agencies to determine (1) if their transaction is likely subject to a CFIUS review, and (2) if so, what national security concerns are implicated and what measures could mitigate those concerns. Forthcoming regulations (2008) will provide examples of transactions that have presented national security considerations.

Parties thus (a) can structure their transaction to better satisfy CFIUS demands, (b) will hopefully have a more reliable expectation regarding the timeframe for concluding the transaction, and (c) can better manage communication of the transaction with shareholders and press, to lessen potential detrimental market perceptions and effects.

III. Initiation of Review

- EITHER A. Any party to a relevant transaction (pending or already completed) may submit a written notice to CFIUS, identifying the transaction. Regulations describe the content required in the notice.
- OR B. Any CFIUS member agency or the US President may:
 - 1. unilaterally initiate review of a relevant transaction;
 - OR 2. unilaterally re-open review of a transaction that has already undergone CFIUS review *if* in the original CFIUS review any party to the transaction (a) submitted false or misleading material, or (b) omitted material information;
 - OR 3. re-open review of a transaction that has already undergone CFIUS review *if* the original CFIUS review resulted in a security agreement or other mitigation measure, and *all* of the following apply:
 - (i). a party to the transaction (or the entity resulting from the transaction) intentionally materially breached the agreement or other mitigation measure;
 - AND (ii). the breach is certified to CFIUS by the member agency responsible for monitoring and enforcing the agreement or other mitigation measure;
 - AND (iii). CFIUS determines that there are no other remedies or enforcement mechanisms to address the breach.

IV. Review

Within 30 days of accepting written notification, CFIUS must review the transaction to determine if it affects US national security. The CFIUS member agencies consider (1) factors specified by Congress (and potentially forthcoming in CFIUS regulations), and (2) other factors implicated by the specific transaction being reviewed (a case-by-case assessment).

continued on next page

TABLE ONE (continued)

V. Investigation

If any one of the following three situations apply, CFIUS must (1) conduct an investigation of the transaction (basically an extended review, to last no longer than 45 days from start of investigation), and (2) take necessary actions in relation to the transaction to protect US national security. NOTE: The requirement for investigations of transactions involving “critical infrastructure” only applies if the transaction could impair national security and such potential impairment has not been mitigated -- thus, the factor of “critical infrastructure” does not impose a situation different from non-critical infrastructure transactions. (Further, the exception of C.1. below also applies to critical infrastructure transactions.)

- ONLY IF A. The lead CFIUS agency recommends *and* the other CFIUS member agencies concur, that an investigation is needed for further review of the transaction.
- OR B. The outcome of the review shows that (a) the transaction threatens to impair US national security *and* (b) the threat was not mitigated during or prior to the review. Traditionally, if only one of the CFIUS member agencies perceives a non-mitigated risk to national security, that one agency’s determination is enough to move to the investigation stage.
- OR C. [*Unless the exception below is met.*] The outcome of the review shows that the transaction could result in the control of any person engaged in US interstate commerce by a foreign government or entity controlled by or acting on behalf of a foreign government.
 - EXCEPTION 1. However, if both the Secretary of the US Treasury (the Chairman of CFIUS) and the designated lead CFIUS agency for the transaction jointly determine that the transaction will not impair US national security, then no investigation is required.

VI. Mitigation and Enforcement

- A. If the review and/or investigation resulted in (1) modifications to the transaction, and/or (2) security agreements between the CFIUS member agency(ies) and the parties to the transaction (or the entity resulting from the transaction), the designated lead CFIUS agency for this transaction is authorized to monitor and enforce the agreements.
- B. If, at the conclusion of the investigation, the transaction is determined to impair US national security, the President may take appropriate action to suspend or prohibit the transaction. The President’s determinations and actions are not reviewable in any court of law. The President may direct the US Attorney General to pursue relief, including divestment, in US Federal courts in order to implement and enforce this authority. However, the President may only exercise the authority under this paragraph if ***both*** of the following apply:
 - ONLY IF A. Based on credible evidence, the President believes that the controlling foreign entity might take action that threatens to impair US national security;
 - AND B. The President believes that, in relation to the transaction, other provisions of law (excluding the International Emergency Economic Powers Act) do not provide adequate and appropriate authority to protect US national security.

REFERENCES

50 U.S.C. App. 2170. Authority to review certain mergers, acquisitions, and takeovers (as amended by the Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246).
CFIUS regulations are found at 31 CFR 800 (note that the published regulations are based on old law; proposed regulations were issued earlier in 2008 but were not published in final form before this article was submitted).
Exec. Order No. 13456, 73 Fed. Reg. 4677 (Jan. 25, 2008).

REFERENCES

¹ Ralph H. Folsom et al., *International Business Transactions*, 2nd ed. (St. Paul, MN: West Group, 2001), § 29.14; see also Edward M. Graham & David M. Marchick, *US National Security and Foreign Direct Investment* (Washington, DC: Institute for International Economics, 2006), p. 20. Graham and Marchick noted that a later congressional hearing evinced testimony that most foreign direct investment into the United States came from Europe, with little being directly invested by Organization of the Petroleum Exporting Countries.

² [Executive Order 11858](#), 3 C.F.R. 990 (1971-1975), *Federal Register*, vol. 40, p. 20263 (May 9, 1975), reprinted as amended in 15 U.S.C. § 78b note (2006).

³ Executive Order 11858.

⁴ Ralph H. Folsom et al., *International Business Transactions*, § 29.14 (noting that under President Carter, only one transaction was investigated).

⁵ In 1970, foreign direct investment amounted to \$13 billion; in 1988, it totaled \$300 billion. Earl H. Fry, “Foreign Direct Investment in the United States: The Differing Perspectives of Washington, D.C. and the State Capitals,” *Brigham Young University Law Review*, vol. 2, p. 372, 1989.

⁶ Ralph H. Folsom et al., *International Business Transactions*, § 29.14 (discussing the attempted acquisitions of Fairchild Semiconductor by a Japanese company and of Phoenix Steel by a company that had Chinese financing).

⁷ Joint Security Commission, [Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence](#), Feb. 28, 1994, p. 70.

⁸ Edward M. Graham and David M. Marchick, *US National Security and Foreign Direct Investment*, pp. 29, 41.

⁹ Ralph H. Folsom et al., *International Business Transactions*, § 29.14.

¹⁰ Edward M. Graham and David M. Marchick, *US National Security and Foreign Direct Investment*, p 41.

¹¹ Named for Senator James Exon and Representative James Florio.

¹² 50 U.S.C. appendix § 2170 (2006) (as amended by the Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246).

¹³ 50 U.S.C. appendix §§ 2170(a), 2170(d) (2006) (as amended).

¹⁴ Executive Order 12661, 3 C.F.R. 618 (1988), *Federal Register*, vol. 54, p. 79 (Jan. 9, 1989), reprinted in 19 U.S.C. § 2901, reprinted as amended in 15 U.S.C. § 78b note (2006).

¹⁵ Edward M. Graham and David M. Marchick, *US National Security and Foreign Direct Investment*, p. 145.

¹⁶ Edward M. Graham and David M. Marchick, *US National Security and Foreign Direct Investment*, p. 29, 145.

¹⁷ National Defense Authorization Act for Fiscal Year 1993, Public Law 102-484, § 837, 106 Stat. 2315, 2463-65; Defense Production Act Amendments of 1992, Public Law 102-558, § 163, 106 Stat. 4198, 4219-20. These quadrennial Critical Technologies Reports must (1) “assess if there is credible evidence that one or more countries or companies have employed a coordinated strategy to acquire United States companies involved in research, development, or production of critical technologies for which the United States (U.S.) is a leading producer;” and

(2) “identify whether there are economic espionage activities directed by foreign governments against private U.S. companies aimed at obtaining commercial secrets related to critical technologies.” *Report on U.S. Critical Technology Companies: Report to Congress on Foreign Acquisition of and Espionage Activities against U.S. Critical Technology Companies*, September 2007 (a [declassified version](#) of December 2006 report), p. 4. The key findings of the 2007 report were: (1) the determination that “[t]here is no credible evidence of a widespread coordinated strategy among foreign governments or corporations to acquire U.S. companies involved in research, development, or production of critical technologies through foreign direct investment;” (2) analysis that showed “that if a coordinated strategy existed, it was not widespread and not economically significant;” and (3) the conclusion that “[f]oreign firms are not concentrating their investment solely in critical technology areas.” *Id.* at 4-5.

¹⁸ U.S. General Accounting Office, “Defense Trade: Mitigating National Security Concerns under Exon-Florio Could be Improved,” September 2002 (GAO-02-736), pp. 2, 8-9, 9 note 7.

¹⁹ See “Foreign Government Ownership Of American Telecommunications Companies,” prepared statement of Larry R. Parkinson, General Counsel, Federal Bureau of Investigation, hearing before the Subcommittee on Telecommunications, Trade, & Consumer Protection of the House Committee on Commerce, 106th Congress, 2000, p. 43.

²⁰ Based on FINSA and its implementing regulations; relevant changes in the 2008 proposed regulations are noted.

²¹ FINSA states that this determination may be made jointly by the CFIUS Chair and designated lead CFIUS agency for the transaction. However, CFIUS has historically acted as a consensus entity. Thus in January 2008, President Bush noted in Executive Order 13456 that CFIUS must initiate an investigation if any member agency deems the transaction to be a unmitigated risk to national security. (*Federal Register*, vol. 73, Jan. 25, 2008, p. 4677).

²² Executive Order 13456.

²³ Executive Order 13456.

²⁴ Edward M. Graham and David M. Marchick, *US National Security and Foreign Direct Investment*, p. 54.

²⁵ 50 U.S.C. appendix, 2170 § (f)(6) (as amended).

²⁶ 50 U.S.C. appendix 2170 § (b)(2)(B)(i)(III) (as amended).

²⁷ 50 U.S.C. appendix §§ 2170(a)(6) (as amended).