



Exon-Florio amendments enacted

President Bush signed legislation amending the Exon-Florio Act that provides for national security review of foreign investments in the US. The legislation is likely to lead to an increase in the number of transactions notified and investigated under the Act as well as increased Congressional involvement in the review process.

On 26 July 2007 President Bush signed legislation¹ amending the Exon-Florio Act (the Act), which provides for national security review of certain acquisitions that are conducted by the Committee on Foreign Investment in the United States (CFIUS). Calls for Exon-Florio reform were prompted by controversies that erupted over some recent transactions, including the proposed acquisition of certain US ports by Dubai Ports World, a UAE government controlled entity, and certain energy assets by CNOOC, a Chinese government controlled entity.

The new legislation (a) explicitly expands and clarifies the definition of 'national security', (b) makes the review process more rigorous and in certain circumstances longer, (c) outlines more precisely the participation and duties of various government agencies, (d) imposes on CFIUS expanded Congressional reporting obligations, and (e) for the first time provides for civil penalties for certain violations. The legislation is likely to lead to an increase in the number of transactions notified and investigated under the Act.

Summary of the Exon-Florio Act

Originally enacted in 1988, the Act grants the President the authority to review and suspend or prohibit acquisitions, mergers or takeovers by foreign persons of persons engaged in US interstate commerce if such transactions threaten to impair the national security of

¹ Foreign Investment and National Security Act of 2007 (H.R. 556).

the US. To exercise this authority, the President must find that (i) there is credible evidence that a 'foreign interest exercising control might take action that threatens to impair the national security,' and (ii) other laws do not, in the President's judgement, 'provide adequate and appropriate authority' to protect the national security. The voluntary review process is initiated by filing a notice with CFIUS, an inter-agency committee comprised of representatives of executive agencies chaired by the US Treasury Secretary. After an initial 30-day review period, CFIUS can initiate a 45-day investigation; if it does so, it must report its final determination as to whether the transaction may affect national security to the President. The President then has 15 days to take any action and must submit to Congress a written report of the decision.

Expansion of national security considerations

The Act had never defined national security; it only provided a list of factors that could be considered by CFIUS and the President.² Although the prior list was never considered exhaustive, the new legislation

² The original factors included: (a) domestic production needed for projected national defence requirements; (b) the capability and capacity of domestic industries to meet national defence requirements, including the availability of human resources, products, technology, materials and other supplies and services; (c) control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the US to meet the requirements of national security; (d) potential effects of the transaction on sales of military goods, equipment or technology to any country identified by the Secretary of State as a country that either supports terrorism, or is a country of concern regarding missile, chemical or biological weapons proliferation; and (e) potential effects of the transaction on US technological leadership in areas affecting national security.

(a) makes consideration of the factors mandatory and (b) enumerates and provides some definition to a number of factors that were thought to be considered in practice, but were not explicitly identified, including:

- the potential for national security-related effects from the acquisition of US critical technologies and/or infrastructure, including energy;
- whether the transaction involves a foreign government controlled entity, and, if so, the foreign country's adherence to non-proliferation policies, counter-terrorism co-operation, and export control record; and
- the potential effects of the transaction on sales of military goods, equipment, or technology to a country that poses a potential regional military threat to the interests of the US.

The legislation provides some guidance to limit what constitutes critical infrastructure by referencing the US Department of Homeland Security (DHS) critical infrastructure paradigm³ and borrowing language from the USA Patriot Act to describe critical infrastructure as those 'systems and assets whether physical or virtual so vital to the US that the incapacity or destruction of such systems or assets would have a debilitating impact on national security.' Critical technologies are defined as 'technology, components, or items essential to national defense.'

Expansion of reviews and investigations

The legislation keeps intact the voluntary nature of notifications submitted to CFIUS pursuant to the Act as well as the prior timing arrangements applicable to such submissions, although the filing entity's chief executive officer (or designee) will now be required to certify that the notification is accurate, complete, and in compliance with regulations.

The legislation also leaves intact the ability of the President or CFIUS to initiate a review of a transaction on their own authority but expands that ability to permit the re-review of transactions involving (a) false statements/omissions of a party or (b) an intentional

³ The DHS identifies the following sectors as critical infrastructure sectors: agriculture, food, water, public health, emergency services, government, defence industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, and postal and shipping, as well as key assets (eg national monuments) and cyber infrastructure.

material breach of a mitigation agreement, provided the breach is certified as such by the Lead Agency (discussed below) and all CFIUS members find there are no other remedies available to address the breach. This 'evergreen' provision would leave transactions that have received clearance, once the primary benefit of making a voluntary notification, open to future Presidential action.⁴

The legislation retains the requirement that a 45-day investigation be undertaken of transactions that 'threaten to impair' US national security where the threat has not been mitigated. However, the legislation now (a) makes mandatory an investigation of all transactions involving a foreign government controlled entity and (b) requires an investigation of transactions involving critical infrastructure of or within the US that 'could impair' US national security where the threat has not been mitigated. Both of these requirements can be waived if the US Department of the Treasury and the Lead Agency (discussed below) agree. CFIUS also has the discretion to undertake a 45-day investigation if it is recommended by the Lead Agency and CFIUS concurs.

Participation and duties of member agencies

The legislation codifies the membership of CFIUS to include the US Secretaries of Treasury, Homeland Security, Commerce, Defense, State, and Energy, as well as the Attorney General. It also codifies the chairmanship in the US Secretary of the Treasury. The President is permitted to appoint other executive branch representatives as deemed appropriate. The US Secretary of Labor and Director of National Intelligence (DNI) will now serve as non-voting ex officio members. The DNI is tasked with submitting a report of the associated national security risks within 20 days of any notification.

In practice, CFIUS generally operated by consensus and, on a given transaction, the agency considered to have the most at stake was appointed as the lead agency. The legislation codifies that practice by requiring the US Department of the Treasury to appoint a Lead Agency(ies) and to delegate to that agency the ability to enter into any necessary mitigation agreements, on behalf of CFIUS, with the parties to a transaction.

⁴ Previously, breaches of mitigation agreements would have been addressed through litigation or, potentially, debarment from government contracting.

The Lead Agency is then tasked with monitoring and reporting on compliance with the mitigation agreement. Mitigation agreements had been standard practice, and the legislation now codifies the authority of the CFIUS agencies to enter into and enforce these agreements. Any such mitigation agreement must 'be based on a risk-based analysis of the threat to national security of the transaction', a standard not previously imposed.

Penalties for non-compliance

The Act previously did not include penalties for non-compliance other than the threat of future Presidential action against a non-notified transaction. The new legislation provides for civil penalties for violations of the Act and/or any mitigation agreement. Subsequent regulations will define the nature and extent of potential penalties.

Additional congressional reporting requirements

Members of Congress often criticised the failure of CFIUS to consult adequately with Congress during reviews and to submit statutorily required reports. The reform legislation imposes new reporting obligations to ensure Congressional consultation during reviews, in addition to the regular annual reporting previously required. The annual report will now have to include a section on critical technology. Additionally, a special report must be issued regarding all reviewed transactions that raised national security considerations, including an assessment of all investments in critical infrastructure by foreign government controlled entities or persons of foreign countries that (a) participate in the Israel boycott and/or (b) do not ban organisations designated as foreign terrorist organisations.

Conclusion

The codification of certain CFIUS practices will bring greater clarity to the process and the procedure for obtaining clearance. The new legislation also addresses Congressional interest in having greater oversight and transparency. However, given that the notification provisions remain largely voluntary, assessments of the applicability of the statute and risks associated with

not submitting a notification remain with the parties to a transaction. The explicit expansion of factors to be considered during an investigation is likely to increase the chances that a party will decide to notify, and, once that notification is made, the chances of a 45-day investigation being instituted are higher. The codification of mitigation agreements and implementation of penalties are likely to increase the formality of what had been a somewhat informal negotiation process.

Going forward, parties will need to think more expansively about the applicability of the statute, the participation of foreign government controlled entities and the potential dynamics and implications of negotiating any mitigation agreements. This legislation puts an even greater premium on ensuring that any acquisition checklist includes the timely development of a thorough strategy for addressing the national security aspects of a transaction, both from a Congressional (ie political) and Executive Agency perspective.

For further information please contact	MJ Moltenbrey T + 1 202 777 4560 E mj.moltenbrey@freshfields.com
	Bob Schlossberg T + 1 202 777 4550 E robert.schlossberg@freshfields.com
	Paul Yde T + 1 202 777 4530 E paul.yde@freshfields.com
	Freshfields Bruckhaus Deringer LLP 701 Pennsylvania Avenue, NW Suite 600 Washington, DC 20004-2692 T + 1 202 777 4500 F + 1 202 777 4555