US COMMERCE DEPARTMENT FORECASTS INCREASED NATIONAL SECURITY CONTROLS ON EMERGING TECHNOLOGY

On 19 November 2018, the US Department of Commerce's Bureau of Industry and Security (BIS) issued an important notice of proposed rulemaking (ANPRM) as the first step in expanding US export and foreign investment controls to cover a range of emerging technologies deemed critical to US national security in the coming decades. The ANPRM identifies fourteen technology areas which may be subject to increased export and investment restrictions, and solicits public comments on how those technologies should be identified and controlled going forward. Comments on the ANPRM are due by 19 December 2018.

Key issues

- The US Department of Commerce has issued an advanced notice of proposed rulemaking with respect to identifying emerging technologies that should be subject to increased export and investment controls.
- The notice identifies 14 technology categories that may be subject to increased controls, and asks the public to comment on how emerging technologies in those fields should be identified for control.
- Comments on identifying emerging technologies are due by 19 December 2018.

BACKGROUND

"Emerging" technologies are poised to change the world over the next decade. Driverless cars, biotech, 3D printing, robotics and artificial intelligence (to name just a few) promise to transform how we live and work. More and more, they will also transform how state and non-state actors project power, and how they protect themselves against national security threats. Most of these technologies began as civilian concepts, with military or national security applications developing only gradually. Because they did not present clear national security issues at first, emerging technologies such as artificial intelligence, autonomous vehicles and biotechnology have not been subject to significant national security controls in most cases.

In recent years, the US Government has become increasingly sensitive to how US national security may become dependent on these emerging technologies in the medium to longer term. The US Congress enacted both the Export Control Reform Act (ECRA) and the Foreign Investment Risk Review Modernization Act (FIRRMA) in August 2018 in response to these concerns. ECRA authorises BIS to establish additional export controls on emerging and foundational technologies that do not currently face significant control but which are deemed critical to US national security in the future. FIRRMA empowers the Committee on Foreign Investment in the United States (CFIUS) to apply additional restrictions on non-US investment in US companies involved in those fields.

Under ECRA, emerging technologies with national security implications will be identified through an interagency process led by BIS, and subjected to additional controls under the US Export Administration Regulations (EAR) and CFIUS review under FIRRMA. The process defined in ECRA will consider the specific national security concerns raised by each technology, including the nature of the technology and its applications, its availability outside the United States, the effect export controls may have on its development in the United States, and whether export controls can limit proliferation abroad.

The ANPRM is a key part of that process as the US Government considers which emerging technologies merit additional restrictions. Such restrictions could include limits on the export of end products and the use of non-US engineers, more extensive CFIUS reviews for inbound investment, reduced access rights for non-US investors, new barriers to international collaboration, and additional administrative burdens for US companies and research institutions. BIS does not seek to expand jurisdiction over “fundamental research" or other areas excluded from EAR control, nor does it express any intention to alter existing controls on technology already specifically controlled in the EAR. It does seek to expand the level of controls applied to emerging technologies previously subject to only limited control, however.

Such increased controls could impact US and non-US institutions across a broad array of industries and disciplines. For example, car companies developing autonomous vehicle capabilities could face additional controls on cross-border collaboration in autonomous navigation; universities researching applications for synthetic biotechnology or advanced computing could be required to exclude certain graduate students from those programmes based on nationality; and financial institutions incorporating face or voice recognition or natural language processing into their customer support systems could face new licence requirements to export those systems outside the United States or transfer them between third countries.

TECHNOLOGIES UNDER SCRUTINY

The ANPRM has three clear objectives. First and foremost, BIS intends to signal the US Government's interest in expanded export controls on technologies within the fourteen fields identified in the notice. These technologies are already subject to the EAR, in that their export to a small number of sanctioned countries and for certain end uses and to certain end users is restricted. BIS is now considering a much broader range of controls that could restrict how companies develop and deploy them. The fourteen fields being considered are:

1. **Biotechnology**, such as: (i) Nanobiology; (ii) Synthetic biology; (iii) Genomic and genetic engineering; and (iv) Neurotech;

2. **Artificial Intelligence** (AI) and machine learning technology, such as: (i) Neural networks and deep learning (eg brain modelling, time series prediction, classification); (ii) Evolution and genetic computation (eg genetic algorithms, genetic programming); (iii) Reinforcement learning; (iv) Computer vision (eg object recognition, image understanding); (v) Expert systems (eg decision support systems, teaching systems); (vi) Speech and audio processing (eg speech recognition and production); (vii) Natural language processing (eg machine translation); (viii) Planning (eg scheduling, game playing); (ix) Audio and video manipulation technologies (eg voice cloning, deepfakes); (x) AI cloud technologies; or (xi) AI chipsets;

3. **Position, Navigation and Timing** (PNT) technology, such as advanced applications for GPS or other satellite navigation signals;
4. **Microprocessor technology**, such as: (i) Systems-on-Chip (SoC); or (ii) Stacked Memory on Chip;
5. **Advanced computing technology**, such as: (i) Memory-centric logic;
6. **Data analytics technology**, such as: (i) Visualisation; (ii) Automated analysis algorithms; or (iii) Context-aware computing;
7. **Quantum information and sensing technology**, such as: (i) Quantum computing; (ii) Quantum encryption; or (iii) Quantum sensing;
8. **Logistics technology**, such as: (i) Mobile electric power; (ii) Modelling and simulation; (iii) Total asset visibility; or (iv) Distribution-based Logistics Systems (DBLS);
9. **Additive manufacturing** (eg 3D printing);
10. **Robotics**, such as: (i) Micro-drone and micro-robotic systems; (ii) Swarming technology; (iii) Self-assembling robots; (iv) Molecular robotics; (v) Robot compilers; or (vi) Smart Dust;
11. **Brain-computer interfaces**, such as: (i) Neural-controlled interfaces; (ii) Mind-machine interfaces; (iii) Direct neural interfaces; or (iv) Brain-machine interfaces;
12. **Hypersonics**, such as: (i) Flight control algorithms; (ii) Propulsion technologies; (iii) Thermal protection systems; or (iv) Specialized materials (for structures, sensors etc);
13. **Advanced Materials**, such as:(i) Adaptive camouflage; (ii) Functional textiles (eg advanced fiber and fabric technology); or (iii) Biomaterials; and
14. **Advanced surveillance technologies**, such as (i) Faceprint; and (ii) Voiceprint technologies.

In addition to identifying these fourteen fields of heightened concern, the ANPRM requests comments from industry and other parties on how those fields could be better defined and controlled. The specific areas identified for comment include:

- How to define emerging technology to assist identification of such technology in the future;
- Criteria to determine whether specific technologies within these general categories are important to US national security;
- Sources to identify such technologies;
- Other general technology categories that warrant review;
- The status of development of these technologies in the United States and other countries;
- The impact specific emerging technology controls would have on US technological leadership; and
- Any other approaches to the issue of identifying emerging technologies important to US national security, including the stage of development or maturity level of an emerging technology that would warrant consideration for export control.

Finally, by giving only 30 days for interested parties to comment on the ANPRM, the US administration is signalling both how urgently it perceives the threat and how difficult establishing meaningful export controls on emerging technologies is likely to be. It plans to proceed at a pace, but recognises the issues in defining emerging technologies such as AI and autonomy in ways that contain proliferation but don't hamper US innovation, which is often dependent on the free exchange of ideas between academic and commercial environments and across borders. The administration's answer to these challenges is likely to influence in significant ways how US industry and research institutions finance, staff, develop and market emerging technologies for years to come. These efforts will almost certainly affect the export control regimes in Europe, Asia and elsewhere as well through multilateral regimes such as the Wassenaar Arrangement.

CONCLUSIONS

The ANPRM published last week is the first chance for US industry, research institutions and the public to see and provide input on how the United States intends to address the national security implications of emerging technologies for the foreseeable future. Companies, investors, academic institutions and dealmakers across a range of industries both inside and outside the United States will likely be impacted by this effort.

Companies exposed to any of the technologies at issue should consider making their voices heard during the consultation period and afterwards. We would encourage any party involved in the development or use of emerging technologies to consider how the ANPRM might impact their activities, and to submit comments by 19 December as the best way to improve the outcome.

Equally important, we would urge them to stay engaged after 19 December, as the process initiated by the ANPRM will likely continue through much of 2019 and beyond. The outcome of this ANPRM is likely to shape national security controls on emerging technologies imposed by the United States and (through multilateral regimes) many other countries for the next decade or more. Companies and institutions with an interest in how emerging technologies are controlled should make their voices heard, to avoid being left out of this important debate.

CLIFFORD
CHANCE

CONTACTS

Joshua Berman
Partner

T +1 202 912 5174
E joshua.berman
@cliffordchance.com

David DiBari
Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

Ling Ho
Partner

T +852 2826 3479
E ling.ho
@cliffordchance.com

Wendy Wysong
Foreign Legal Consultant (Hong Kong),
Partner
(Washington, DC)

T +852 2826 3460
+1 202 912 5030
E wendy.wysong
@cliffordchance.com

Joshua Fitzhugh
Counsel

T +1 202 912 5090
E joshua.fitzhugh
@cliffordchance.com

Lei Shi
Consultant

T +852 2826 3547
E lei.shi
@cliffordchance.com

Michelle Williams
Counsel

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Nicholas Turner
Registered Foreign Lawyer

T +852 2825 8854
E nicholas.turner
@cliffordchance.com

Ekaterina Hazard
Associate

T +1 202 912 5027
E ekaterina.hazard
@cliffordchance.com

Laurence Hull
Associate

T +1 202 912 5560
E laurence.hull
@cliffordchance.com

Hena Schommer
Associate

T +1 202 912 5447
E hena.schommer
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 27th Floor, Jardine House, One Connaught Place, Hong Kong

Clifford Chance

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.