THE CHINA QUESTION

China has set its sights on being the world leader in technology by the year 2025, an ambition that seriously worries the US government. Among the latter's various responses to the challenge have been a raft of regulations, sanctions and export controls designed to slow the PRC's progress. *WorldECR* examines what it all means for business.

Companies all over the world are finding themselves caught in a minefield of US and international regulations, as Washington and its allies lay down export controls and sanctions to slow Beijing's advance toward its goal of seizing global dominance from the United States in technology, trade and military might.

The impact of US and EU trade controls, sanctions and related regulations – combined with the effects of the Covid pandemic – has rolled like a temblor across the globe, shaking up international supply chains in sectors from textiles and agriculture to the auto industry and semiconductors. Many businesses worldwide have been forced to shift down, shut down, or shuffle suppliers.

Companies have been especially impacted by the raft of trade regulations that were pumped out under President Trump and which have continued with the Biden administration (see following pages). These target mainly China and are aimed at

blocking the country from accessing US technology and innovation that could help Beijing get ahead in security, defence, and economic standing.

With space and cyberspace seen as the modern battlefields where the fight for global supremacy will be won or lost, the United States has built a wall of sanctions and regulations to stop China from gobbling-up its technology. This has thrust technology and hi-tech companies everywhere – especially in the United States – into the front lines of the US-China battlefield. It's a shifting area whose rules and boundaries are not always clearly defined.

Start-ups and shut-downs

Brian Egan, a partner at law firm Steptoe & Johnson LLP in Washington, DC, says that while many global giants and other large companies have the in-house expertise to understand how they are impacted by the wave of new regulations, others often do not.

'You have some smaller tech start-up companies that might be in what I call "the clueless phase," or the "ignorance is bliss phase", where they have some sense that they may face some obstacles, but they don't necessarily realise how a partnership with a Chinese company could lead to regulatory complications,' Egan says. 'Then you have some tech companies that see dark clouds on the horizon and want to do something but they're not sure what to do.'

Largely, these businesses are left in limbo because the Biden administration has taken no steps to suspend or roll back some very important Trump-era regulations relating to China trade that have a very broad impact, but are very unclear.

Egan says that one example is the Information and Communications Technology Services ('ICTS') rule, which, by the Commerce Department's own estimate, potentially affects up to 4.5 million US businesses.

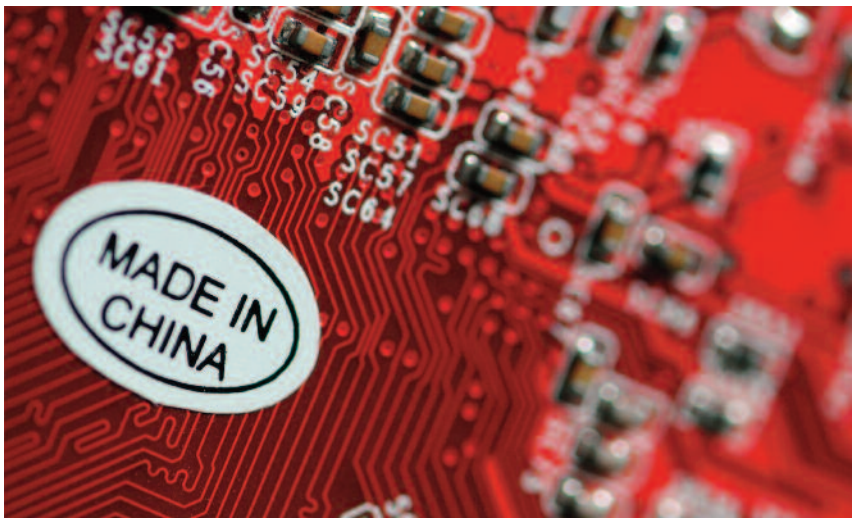
'The regulation has been put in place on the information and communications technology supply chain, where the US essentially has said, "We reserve the right to prohibit any transactions involving the US telecommunication supply chain and China,"' Egan explains. 'But the US government hasn't told anybody which transactions they will prohibit, there's no mechanism for seeking approval or clearance, and the US government has given itself the right to retroactively prohibit transactions that have already been consummated. That's kind of like saying, "We'll let you know if we see a transaction that's problematic," but by the time a company hears from the US government it may be too late – the transaction may have already taken place. So, even if a company wants to comply with this and be consistent with US policy, it's very difficult for companies to figure out what to do.'

'The US government has given itself the right to retroactively prohibit transactions that have already been consummated.'

Brian Egan, Steptoe

Then-President Trump declared an ICTS threat emergency when, in May 2019, he signed an executive order ('EO') that effectively banned Chinese telecoms giant Huawei from receiving semiconductors made with US technology. Later, in August 2020, he banned the popular Chinese-owned apps TikTok and WeChat in the United States, citing concerns over the swaths of personal data of Americans that would be in the hands of Chinese companies, including location data and internet search histories. Trump said that was a national security risk – companies would have no choice but to hand their data over to the Chinese government if asked.

But the bans on TikTok and WeChat never took effect because they were blocked



Made In China 2025

The Made in China 2025 plan was released in 2015. It put into writing the Chinese government's ambition to move the country from low-value manufacturing, reliant on cheap labour, by becoming a leader in higher technology and, with that, the world's leading manufacturer of semiconductors. Ten sectors were identified as key to realising the ambition:

1. **New generation information technology**
2. **Advanced numerical control machine tools and robotics**
3. **Aerospace technology, including aircraft engines and airborne equipment**
4. **Biopharmaceuticals**
5. **High-performance medical equipment**
6. **Electrical equipment**
7. **Farming machines**
8. **Railway equipment**
9. **Energy-saving and new energy vehicles**
10. **Ocean engineering**

Biden administration continues Trump's legacy of trade control restrictions on China

Since taking office in January 2021, the Biden administration has continued the Trump administration's legacy of expansive US national security restrictions on China, *writes Ajay Kuntamukkala, a partner in the DC office of law firm Hogan Lovells*.

While the Biden administration has adopted a more measured tone and has sought the cooperation of traditional US allies, it has signaled that it intends to continue a robust approach to countering perceived national security threats from China. Rather than reversing course, the Biden administration has doubled down on the Trump aministration's aggressive national security policies related to China, which included executive orders, regulations, and other measures imposing restrictions on the transfer of technology and items to China and Hong Kong; prohibiting investments and other activities involving Chinese parties associated with the Chinese military and intelligence establishment; prohibiting transactions involving China that pose a threat to US supply chains and information and communications technology infrastructure (including certain Chinese apps); and sanctioning specific parties involved in human right abuses, undermining democracy in Hong Kong, and the ongoing fusion between the civil and military sectors in China, among others.

As shown in Figure 1, the Trump administration and now the Biden administration have taken a broad and robust approach to countering national security threats from China by leveraging a large number of policy tools and agencies. Known as the 'whole of government' approach, the US government has imposed restrictions covering export controls, economic sanctions, customs, investment and securities restrictions, immigration, national security tariffs, IP theft prosecutions, and other measures. A number of agencies have been involved, including the US Trade Representative and departments of Commerce, State, Treasury, Defense, Homeland Security, and Justice/FBI.

Figure 2 depicts the escalating pressure on China through key national security measures imposed on China using presidential executive orders and actions by the White House and specific agencies, including the Departments of Commerce, Treasury and Defense. These efforts began to take shape in parallel with the US-China trade talks and broader tensions resulting from Covid-19, China's National Security Law, and Xinjiang province.

Taken as a whole, the Biden administration's national security approach to China represents a continuation of President Trump's policy shift from accommodating China to confronting China directly in an attempt to impose costs on Chinese behaviour that threatens US interests. A major component of this strategy has been to expand national security restrictions on activities involving China, including export controls, sanctions and other measures.

Figure 1. Current US national security toolkit

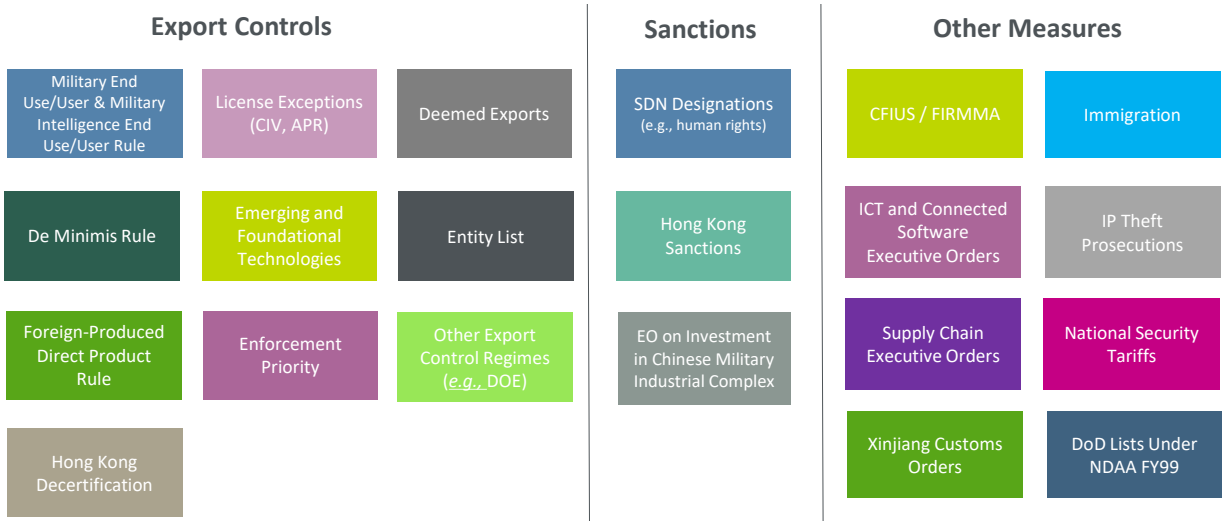
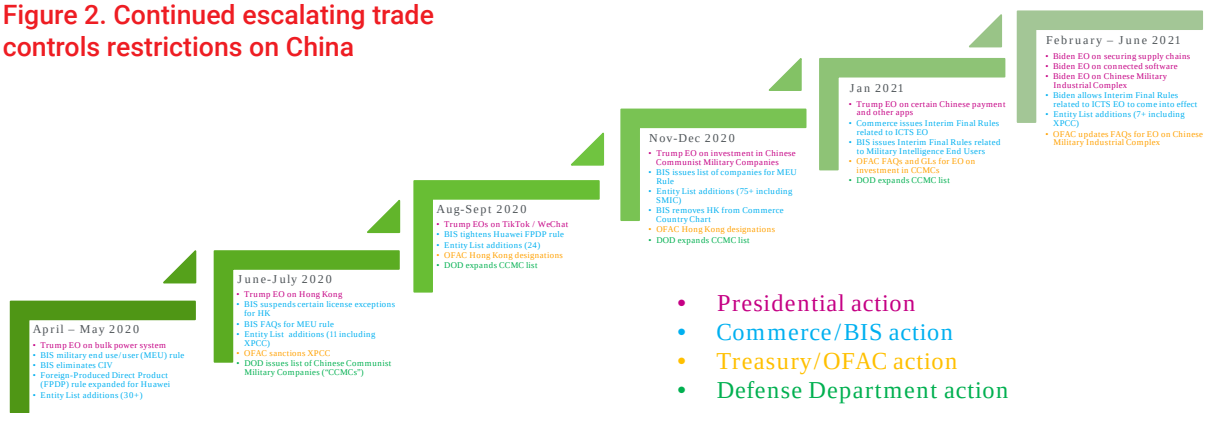


Figure 2. Continued escalating trade controls restrictions on China



Source:Hogan Lovells

by US courts and on 9 June President Biden issued a new EO revoking the string of orders his predecessor signed to target TikTok, WeChat and eight other China-linked apps. President Biden's EO instructs the Commerce Department to launch a new review to identify possible security threats from those apps and others.

'The Military Intelligence End-User rule applies to all products that are subject to US export controls, even the least sensitive, EAR99 products.'

Tahlia Townsend, Wiggin and Dana

Because of its ambiguity and potential reach, there was speculation as to whether Biden would make adjustments to the powerful ICTS tool handed to him by Trump. Companies and compliance lawyers have been keeping a close watch on the current administration to understand how it intends to enforce many of the Trump-era regulations targeting China.

On 26 March, the Commerce Department said it wanted fresh public input on establishing licensing or other procedures to help companies comply with the ICTS rule. But it made that announcement four days after allowing Trump's interim ICTS regulations to automatically come into force. Even before they officially came into effect, Commerce Secretary Gina Raimondo disclosed on 17 March that subpoenas had been served on multiple Chinese companies that provide ICTS services in the United States. Businesses and compliance experts saw that as an indication of the vigour with which the Biden administration is expected to go forward on China.

'We are seeing upward trends in sanctions and export controls both in the US and the EU,' Egan says. 'The Biden administration has so far continued an aggressive use of these tools, which leads to a very complicated regulatory landscape for companies doing business on both sides of the Pacific Ocean.'

But he advises that businesses should be looking at 'compliance opportunities'.

'In a lot of the regulations there's at least limited room for continued activity or for authorisations for activities that may be otherwise prohibited. For example, a US company that is doing business with a Chinese party that's been added to the US Entity List may say to itself, "What can I continue doing today in compliance with US law, and what could I seek approval to do, even if it's not authorised, but where I think the US government actually may not have a problem with me continuing certain activities?"' Egan explains.

Meredith Rathbone, also a partner at Steptoe, advises that in this uncertain terrain companies should be engaging in 'a compliance-mapping exercise, so that if new restrictions come into place companies are ahead of the game in identifying pressure points.' She says this would give companies 'an opportunity to quickly assess whether or not they can proceed with business as usual.'

Rathbone notes that one of the biggest challenges companies face now is monitoring all the changes and anticipating future ones. 'We're getting more and more requests to monitor what's going on and what might happen next, not just actual pieces of legislation or regulation but things like: What are key members of Congress doing? What are key members of the administration saying? Who's been appointed to which position and what's perspective?'

In the US Congress, the mood of Biden's fellow Democrats about China can perhaps be gleaned by the EAGLE Act ('Ensuring American Global Leadership and Engagement', see box below). The bill was introduced on 25 May by Gregory W. Meeks (D-NY), chairman of the House Committee on Foreign Affairs. The 470-page legislation calls for 'the revitalization of American diplomacy, leadership, and investments globally in response to the policy challenges posed by China.' Among other things, it seeks increased investment to promote US manufacturing, working with allies on China policy, re-engagement in international organisations and recognition of China's treatment of its Uyghur Muslim minority as genocide.

Mao's vision: 'surpass the US'

'Given 50 or 60 years, we certainly ought to surpass the United States,' China's revolutionary leader Chairman Mao said in a 1956 speech. 'To surpass the United States is not only possible, but absolutely necessary and obligatory,' he ordered.

That duty has not been lost on President Xi Jinping, who has laid out the same objective for Chinese tech: 'catch up and surpass' the United States in global leadership.

The goals of 'Made in China 2025', the 10-year plan launched by the Chinese Communist Party ('CCP') in 2015, include leaving the United States and the world behind in key technologies, from next-generation wireless networks to artificial intelligence.

On 10 June, US Secretary of Defence Lloyd Austin issued an internal directive to 'laser focus' US military 'efforts to address China as the nation's number one pacing challenge.'

EAGLE Act: key elements

- 'Emphasizes the power of multilateralism and boosts American leadership in international organisations such as the United Nations, as well as regional ones like APEC;
- Reinforces US commitment to engagement with partners and allies through bilateral and trilateral engagement as well as through the Quadrilateral Dialogue;
- Spurs US strategic and economic competitiveness on the world stage through climate action, vaccine diplomacy, development finance, and digital and cyber partnerships;
- Holds China, the world's largest emitter of greenhouse gasses, accountable on climate, to ensure that it plays a constructive role in the climate fight;
- Reinforces commitment to American values by responding to the PRC's human rights violations, imposing costs on China for its use of Uyghur forced labour, and providing temporary protected and refugee status for qualifying Hong Kongers; and
- Strengthens America's economic diplomacy and statecraft in order to shape the economic rules that govern global commerce, empower American workers and businesses, and invest in the technologies of the future.'

Amongst its many sanctions-related provisions, the act calls upon the President to urge the United Nations Security Council to invoke 'multilateral sanctions' against China for 'genocide and crimes against humanity against Uyghurs and members of other ethnic and religious minority groups'.

The State Department warned that China intends to become a tech leader 'not just through its own research and development efforts, but also by acquiring and diverting the world's cutting-edge technologies – including through theft – in order to achieve military dominance.'

To disrupt that process, among other steps, the United States has expanded its Entity List, created a Military End User ('MEU') list and, in March this year, introduced the Military Intelligence End User ('MIEU') Rule (see box, opposite). Some of those regulations extend to other countries as well, but they mainly target China and aim to curtail its access to certain US hi-tech.

Tahlia Townsend, a partner at the law firm of Wiggin and Dana, says that the end-user rules have had 'a very large impact on both US and non-US companies'.

Since the MEU Rule came into effect in June 2020, the Department of Commerce's Bureau of Industry and Security ('BIS') has relied on companies to carry out their own due diligence to determine whether their potential clients fall under the new rules.

Townsend explains that BIS provides a list of military end-users, which is not all-inclusive. 'So if a party is engaged in activities that would make them a military end-user, even though they are not on the list, the rule still applies,' she explains. 'That has been the big challenge for companies: to try to figure out which Chinese entities are and aren't military end-users. Further, the scope of the rule is very broad and covers a broad range of technologies that would normally not be controlled for exports to China.'

'By way of example, it even applies to two very common software products – Microsoft Excel and Microsoft Word – because they have the ability to encrypt information for confidentiality purposes. As you'd expect, normally those products can be very, very widely exported, but even they are subject to the MEU Rule,' Townsend explains.

'That breadth creates a big headache for non-US companies, too. For example, if you have a foreign software company that makes entirely foreign-origin software but then packages its software with Microsoft products or Java products that are useful to operate the foreign software, that foreign software company has to check whether any of the parties to which it is selling might be considered military end-users by the US government. That is very, very challenging,' she says.

Townsend adds that the heavy additional burden imposed by the various new regulations impacting China,

The Military-Intelligence End Use Rule

On 15 January 2021, the US Bureau of Industry and Security ('BIS') published a rule under the Export Administration Regulations ('EAR') with new restrictions targeting 'military-intelligence end uses/end users' ('MIEU').[1]

The MIEU Rule prohibits the export, reexport, and in-country transfer of any items subject to the EAR – as well as certain support services provided by US persons – to users engaged in intelligence activities for the militaries of China, Russia, Venezuela, and certain other countries.

This MIEU Rule is related to, but distinct from, BIS's 'military end use/end user' ('MEU') Rule. Together, they present challenges for exporters in the US, and reexporters and transferors outside the US.

Summary of the new rule

The MIEU Rule amends the EAR to impose a licensing requirement, effective 16 March 2021, for certain activities involving MIEUs.

Newly added §744.22 restricts any item (i.e., commodity, software, or technology) that is 'subject to the EAR', including those designated as EAR99, where there is 'knowledge'[2] that the item is intended, entirely or in part, for a 'military-intelligence end use' or a 'military-intelligence end user' in China, Russia, or Venezuela or a country listed in Country Groups E:1 or E:2 (currently, Cuba, Iran, North Korea, and Syria).

Defined at §744.22(f)(2), a 'military-intelligence end user' means 'any intelligence or reconnaissance organization of the armed services (army, navy, marine, air force, or coast guard); or national guard,' and provides a non-exhaustive list of agencies related to restricted countries.

The term 'military-intelligence end use' is defined at §744.22(f)(1) to cover the design, 'development,' 'production,' use, operation, installation (including on-site installation), maintenance (checking), repair, overhaul, or refurbishing of, or incorporation into, items described on the US Munitions List or classified under Export Control Classification Numbers ('ECCNs') ending in 'A018' or under '600 series' ECCNs – when those items 'are intended to support the actions or functions of a [MIEU].'

These export, reexport and in-country transfer licensing requirements restrict 'items subject to the EAR', and thus apply to both US and non-US persons.

Amended §744.6(b)(5) prohibits US persons[3] from providing any 'support' to any restricted MIEU without a BIS licence. The definition of 'support' is broad, such as shipping or transferring any items, or performing any 'contract, service, or employment,' with knowledge items may be used in or by, or assist or benefit, a MIEU. Notably, this US person support prohibition applies to items that are not subject to the EAR.

A BIS policy of denial applies to any license applications involving MIEUs.

MEU Rule: not to be confused

The MIEU Rule is different from the MEU Rule, which BIS published in June 2020. The MEU Rule imposes a licensing requirement on the export, reexport, and in-country transfer of certain ECCNs (i.e., not EAR99 items) described in Supplement No. 2 to Part 744, when destined to either a 'military end user' or a 'military end use' in China, Russia, and Venezuela (only). In December 2020, BIS published a non-exhaustive list of end users under the MEU Rule.[4]

Due diligence

BIS recommends exporters utilise Supplement no. 3 to part 732 – BIS's 'Know Your Customer' Guidance and Red Flags to conduct due diligence for parties identified as, or representing a risk of diversion to, prohibited end users/uses. In practice, it may be difficult to ascertain whether items subject to the EAR are 'intended to support the functions' of MIEUs and will require a licence. Reexporters of items subject to the EAR may decide not to supply such items to affected countries. However, given associated US export control risks, BIS would likely expect heightened due diligence, compliance terms and conditions, and other safeguards for exports, reexports, transfers, and US person support services to the affected countries or where a supplier has information that its customer may deal directly or indirectly with MIEUs.

Links and notes

1 On 9 April 2021, BIS published certain technical corrections to the MIEU rule and to add Burma (Myanmar) to the list of countries subject to these export controls. 86 Fed. Reg. 18,433-18,437.

2 'Knowledge' generally means actual knowledge, reason to know, or conscious disregard or wilful avoidance of facts.

3 'US person' generally means any: (1) individual who is a citizen or lawful permanent resident of the US, wherever employed; (2) juridical entity organised under the laws of or within the US, including foreign branches; or (3) person in the US.

4 Supplement No. 7 to Part 744 of the EAR.

By Jack Hayes and Nicholas Turner, Steptoe

including the MEU rule and the restrictions on trade with Huawei, has meant 'a lot of reshuffling of supply chains and a lot of foregone contracts.'

'Regarding Huawei, at first, entities like Qualcomm and Microsoft and others were able to obtain some limited licences from the Department of Commerce,' Townsend says. 'But then, BIS rescinded many of the licences that had been granted and tightened the policy for additional licences. Industry had a real whiplash effect from that, and now you can only really get licences if the products you want to sell will not support 5G technology at all, and even that's not guaranteed.'

As noted above, to make things even more challenging, in March BIS added another layer of difficulty in the shape of the MIEU Rule, which applies to China, as well as Russia, Venezuela, Cuba, Iran, Syria, and North Korea.

'The Military Intelligence End-User rule goes beyond the MEU rule in a couple of ways. First, it applies to all products that are subject to US export controls, even the least sensitive, EAR99 products,' Townsend explains. 'Second, the rule doesn't only apply to transfers of items subject to the EAR (Export Administration Regulations); it applies to any item transferred via a US person, even foreign items, and to any service performed by a US person anywhere in the world that may "assist or benefit" a military intelligence end-user.'

Although the definition of MIEU is narrower than the definition of MEU, it could still have a significant and surprising impact. For example, Townsend refers to news and internet reports and US government agency allegations about major Chinese telecoms companies, including Huawei and ZTE, having close ties to Chinese military and intelligences services.

'With those kinds of allegations in the public domain,' says Townsend, 'if you're a US person anywhere in the world providing services to Huawei or ZTE, even if those items or services don't involve items that are subject to US export control, you have to ask yourself, "If I'm providing services to Huawei or ZTE and I have reason to believe they have provided services to Chinese military intelligence services, is there reason to believe that my services to them are likely to assist or benefit the Chinese military intelligence services?" That's a really, really far-reaching rule. It's much more like a sanctions rule than an export rule.'

A seat at the table for Compliance

Elizabeth Shingler, Tax, Export Controls & Sanctions Manager at KPMG in Philadelphia, observes that, 'There's challenges in industry with the new export restrictions because industry does rely on China. I think the next year or so will be really telling about how things evolve.'

Shingler advises that companies should not wait for the government to clarify regulations and instead should get started early on putting together a robust compliance program. She adds that companies must know everything about their clients and about their products and have it all in one place.

Elizabeth Shingler

'One of the first steps to managing new requirements is assessing what data you have and where it is located,' she explains. 'We see companies struggling to identify the information they need and to validate its accuracy. It's important to identify early who the parties to the transaction are, not just end-users, so risks can be properly assessed.'

She says that the MEU Rule provides the starting point. 'But a process needs to be developed to identify other users who may have a nexus to the military. This can crop up when hospitals, universities or research organisations touch the supply chain. Understanding what ties, if any, there are to the military can take some digging and may require the use of a third-party with local expertise,' she advises.

'Finally, since these regulations are still evolving, incorporating risk assessments into compliance planning will help the organisation stay close to where the risks are and what is driving them, so meaningful compliance steps can be taken,' Shingler says. 'What's nice to see is that businesses are engaging on these topics now and they want to get ahead of it. I think there's a lot of awareness that export compliance is a real issue, not a back office function.'

Shingler adds that for companies, compliance needs to be at the 'forefront of your product-planning process so that licences are in place and people understand that even though they might not sit in compliance, their responsibilities touch export compliance. You kind of have to bring them into the fold and train them on what that means,' she says, 'I think, compared to where we were a few years ago, the level of awareness is very impressive.'

Shingler advises that any company with business that touches China needs to think about the impact from the expanded regulations. 'It's not just multinationals that have to understand where and how you are touching China.'

'As a business, you need a plan for today and you need a plan for tomorrow and you really also need to understand where your business is going and what your relationship with China is going to look like in a few years, so that the export compliance team can start planning for that,' she explains. 'To do that, we need the export compliance teams to start being more a part of the business – not siloed. They need to sit shoulder-to-shoulder with their counterparts in the business so they know what's coming and what looks likely to come, so they can plan appropriately. They need to have a seat at the table.'

No way, Huawei

Huawei became the largest casualty of the US-China hi-tech war when in May 2019 then-President Trump signed an EO banning the Chinese telecoms titan from obtaining semiconductors, including chips made by foreign firms developed or produced with US software or technology. That body blow has not killed Huawei, but it slowed the speed at which the telecoms juggernaut was expanding across the globe.

The Trump administration's core concern with Huawei was over its ties to the Chinese government and fears that its equipment could be used to spy on other countries and companies. In May 2020, a year after the first action against Huawei, Trump extended the ban for another year.

The Biden administration has not reversed Trump's sanctions and tough regulations on China; in fact it has expanded them. On 4 June 2021, President Biden signed an EO banning Americans from investing in dozens of Chinese companies with alleged ties to defence or surveillance technology sectors, including Huawei and SMIC.

Washington has kept up its lobbying with European and other allies to dissuade them from letting Huawei or other Chinese telecoms companies build their next-generation telecoms networks, on grounds the companies could pose a security risk. But small cracks may be appearing in the US global campaign. In late May, British telecoms giant Vodafone's Italian unit received conditional approval in Italy to use Huawei equipment in its 5G radio access network according to news reports. At the World Mobile Congress in Barcelona in late June, Stephane Richard, CEO of Orange, France's largest telecoms firm, told Reuters

that his company will avoid using equipment from Chinese vendors when developing Europe's 5G networks, but sees no issue in working with Huawei in Africa, where the Chinese company dominates as a supplier of equipment to many telecoms operators. Still, a World Bank-led project declined to award a contract to lay sensitive undersea communications cables after Pacific island governments heeded US warnings that participation of a Huawei-linked company posed a security threat, two sources told Reuters on 18 June. The former Huawei Marine Networks, now called HMN Technologies, was part of that project. The news agency quoted two sources with direct knowledge of the tender saying that the project reached a stalemate due to security concerns raised within the island nations over HMN Technologies' bid. The project's planned connection to a sensitive cable leading to Guam, a US territory with substantial military assets, heightened those security concerns.

'Given there was no tangible way to remove Huawei as one of the bidders, all three bids were deemed non-compliant,' one of those sources was reported to have said.

'Whatever approaches companies decide to take with respect to their Chinese partners, they should carefully document their rationale.'

Roy Liu, Hughes Hubbard & Reed

President Trump's 2019 EO targeting Huawei started a chain reaction that has contributed to the current global shortage of semiconductor chips. In Korea, electronics giant Samsung said in May that the chip shortage was affecting television and appliance production and in the United States Ford and General Motors have made massive earnings cuts this year as a result of the chip crisis.

Roy Liu, a partner at law firm Hughes Hubbard & Reed in Washington, DC observes that Chinese companies have reacted in two ways to US export controls that have been increasingly targeting China and to the uncertainty surrounding future restrictions.

'On the one hand, in the short term some of the companies are stockpiling US-origin products or equipment or software or parts and components because of this uncertainty, and that in part has contributed to this current well-known shortage of semiconductor products,' Liu says. 'On the other hand, over the medium and long term, I have observed many Chinese companies that have devised really very thought-out plans about substituting US-origin items with either made-in-China items or items made in other countries,' he adds.

Liu also notes that US and non-US companies face added uncertainties because it is still not very clear how exactly the Biden administration will go about enforcing China-related regulations and restrictions.

'The enforcement actions by the US government have not really kept up with the frantic speed with which those new rules came out,' Liu observes. 'I think for companies, it's really important to carefully analyse and watch for future development and also to carefully analyse the rules that have come up.'

He advises: 'Whatever approaches companies decide to take with respect to their Chinese partners, they should carefully document their rationale and make sure they have the supporting documents, should the US government make any inquiries in the future.'

Ryan Fayhee, Liu's fellow partner at Hughes Hubbard, adds that the expanded regulations mean companies have to devote more time and resources to understanding the end use of their products: 'You're essentially running a diligence exercise on a periodic basis and it puts the need for on-the-ground diligence at a real premium,' he says. 'We've seen vendors willing to do this work, but it increases the cost and the time

Hong Kong story

In July 2020, days before President Trump signed an order formally ending preferential treatment of Hong Kong by the United States, news reports there predicted an expected stampede of US tech companies out of the territory. 'The fallout could be as much as a 30 per cent cut in rents, given that American companies are now the single largest occupier of prime office space in the city,' the English-language *South China Morning Post* commented at the time.

On 14 July 2020, with Trump's signature, Hong Kong's status changed dramatically from a destination to which companies could export a broad range of products, either without a licence or under licence exceptions, to being treated the same as China for all export purposes. Hong Kong became subject to the same Military End-User rule, the later Military Intelligence End-User Rule and also, by default, the highly restrictive export regulations for China, requiring a licence for a very wide range of technologies.

'No special privileges, no special economic treatment and no export of sensitive technologies,' Trump said when he signed the order, two months after his secretary of state Mike Pompeo declared Hong Kong 'no longer autonomous' from China.

The most serious impact from that move was felt by the high-end electronics industry and aerospace companies, which historically had subsidiaries in Hong Kong and had exported to the enclave.

On 3 June, US aerospace giant Boeing's Chief Executive Dave Calhoun referred to the troubled US-China trade relationship, saying he could not predict when a 'thaw out' would open up jet deliveries in one of the world's fastest growing aviation markets.

necessary to secure a transaction in very unusual ways in comparison to anywhere else in the world.'

Fayhee warns that for businesses, 'the risks are real' because BIS has been issuing notifications 'on a far more regular basis than ever before in history.'

Since October last year, BIS has been sending out what have become known as 'is informed' letters to US semiconductor manufacturers via a confidential notice. They are informed that they will require export licences for certain products or technology supplied to Semiconductor Manufacturing International Corporation ('SMIC'), China's largest semiconductor manufacturer.

The *Wall Street Journal*, which broke the story about the notices, said that the Commerce Department was concerned about high risks of diversion to a military end-user. SMIC's customers include US tech giants like Qualcomm, Broadcom and Texas Instruments.

'Companies are well advised to do their diligence at least on a periodic basis, depending upon the nature of the products and the risks,' Fayhee says. 'But they need to be prepared that, in the middle of a supply contract or other obligation, they can receive the "is informed" letter. If they misjudge it and are given this notice, there's nowhere to go from there.'

Diversify, diversify

The landscape for trade with China has changed dramatically in the two decades since President Clinton opened the floodgates of trade with China by championing its entry into the World Trade Organization and granting it most-favoured-nation status, a privilege that was revoked by Trump.

Giovanna M. Cinelli, a partner at law firm Morgan Lewis in Washington, DC, and head of the firm's International Trade and National Security Practice, outlines how the Trump administration used regulations differently to manage what it saw as China's 'threat to the world'.

'The management of key policy and trade issues normally required a focus on the Commerce Department or the State Department, because they handle the majority of activity under US export laws and regulations,' Cinelli explains. 'But the Trump administration utilised a "whole of government" approach to move forward with either sanctions or restrictions. You not only have State and Commerce from the export side, you have the Justice Department focus through the agency's China Initiative, as well as the Federal Communications Commission ('FCC') from the national security side with its designations. In addition, the FBI issued inquiries to industry and the Department of Homeland Security stepped in with restrictions on the basis of cyber-related issues,' she adds.

The Biden administration has continued Trump's policy and recently issued executive orders related to supply chain, protection of personal data, and cyber security. 'That has been a bit of a wrinkle for industry because it's expanded the number of stakeholders in the process and increased the level of engagement that's needed to manage the trading relationship,' Cinelli says, adding that, among other issues, her firm is advising clients to take a detailed look at their partners and their supply chains.

'One of the primary objectives that we're working with clients on is revisiting, updating and re-executing a lot of their commercial documentation. With the review and revision, we're also working with them to diversify their supply chains,' Cinelli adds.

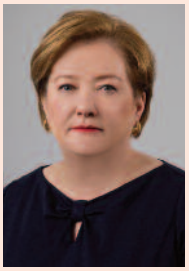
She points out that under Biden, 'The type of objectives that the Trump administration was using to justify a tightening of controls is shifting away from national security alone and towards human rights and foreign policy.

'What we're seeing now in the Biden administration and the EU is an incredible focus on human rights and more foreign-policy-related concerns. We are

Why worry if I don't export?

While corporate giants will likely have the expertise to understand what they can and cannot do under the expanded regulations, it is not always easy for small companies to understand the impact.

'Sometimes clients will ask, "I don't export, so do I need to worry about these regulations?" says Barbara D. Linney, partner at BakerHostetler in Washington, DC, and the firm's International Trade and National Security team co-leader. Linney says that 'the answer to that is "yes", for a variety of reasons,' but advises that a good starting point for all companies dealing in some way with China is the Commerce Department's 'deemed export' rule.



Barbara Linney

'Under the deemed export concept, a release of controlled information to foreign nationals, even if it occurs in the United States, is considered an export,' Linney explains, noting that a product does not have to travel across the US border to be considered an export. 'Just exposing a non-US citizen to export-controlled technology, even on US soil, may be treated as an export,' she says. Such a disclosure of information, if made without a proper licence, is potentially a violation of federal law that could result in harsh penalties.

While the deemed export rule does not apply to China alone, it has a significant impact on transfer of technology to China.

'Companies who are confronted with a multinational workforce, multinational visitors to their plants and so forth obviously have to be aware of these issues, even if they don't send their products or technology out of the United States to another country,' she says.

Linney adds that various players in the supply chain also have become much more sophisticated in terms of requiring their suppliers to provide information, so that they can themselves comply with export control laws and regulations.

'In terms of how to approach advising clients on these issues, you have to make sure the client understands that they have to take a somewhat holistic approach to their compliance system,' Linney says. 'What I mean is that you can't really have your sanctions compliance over here and your export compliance in another place, because if you try to "stovepipe" or separate these functions and these concepts, you can quickly sort of run afoul of rules. You have to think of the whole regulatory landscape and not just look at export controls or sanctions in isolation. You must understand the potential impact of all of the laws and regulations that could impact whatever transaction you're contemplating.'

Classification 'is the foundation of the US export control system,' she says. 'You obviously have to know whether your transaction is subject to ITAR (International Traffic in Arms Regulations) or subject to the EAR (Export Administration Regulations) or subject to other regulatory programs that impact exports. Once you have determined which agency has jurisdiction under which set of rules you also have to know the specific classification in order to drill down and determine whether a licence is required and, if so, what licence exceptions might be available.'

'Without an appropriate export classification effort you simply can't be in compliance with export control laws,' she warns.

anticipating that the restrictions are going to continue and because of that – in addition to revising the commercial documents and working on good documentation – we're working with clients to diversify and find alternative sources. It's not an elimination of China from the supply chain or customer base, but it's a diversification.'

Since 2019, dozens of Chinese officials and companies have been sanctioned or blacklisted by the United States, the EU and the United Kingdom over alleged human rights abuses against Uyghurs and members of other minorities in China's western Xinjiang region.

In January, the United States reacted to allegations of widespread use of forced labour in Xinjiang by banning imports of cotton and other products from the region, with Canada and the UK following suit.

The ban disrupted supply chains across the world: cotton from Xinjiang is among the best in the world and ends up in garments cut and sewn across Asia, from Bangladesh to Vietnam and exported across the world, making it extremely difficult for companies to have full confidence in their supply chains.

'Whatever you have in your supply chain, instead of having only one source you should be trying to find other sources,' Cinelli advises. 'We're seeing this in the semiconductor, telecommunications world, writ large in the financial world,' she observes.

'Whatever you have in your supply chain, instead of having only one source you should be trying to find other sources.'

Giovanna Cinelli, Morgan Lewis

Businesses around the world are trying to manage as best they can with often unclear US regulations, some of them clearly rolled out in haste by the previous administration. □

Introducing Ian Bolton

Ian Bolton is the Editor of FISC. Ian has worked in sanctions compliance for nearly a decade within the UK government, at the Foreign, Commonwealth and Development Office, in academia, at King's College London, and in the banking sector, at HSBC UK. He has written on nuclear proliferation, maritime interdictions, and sanctions compliance for numerous journals (including for WorldECR), and has specialised in delivering sanctions compliance training and capacity building within government, industry and academia – ***ian.bolton@worldecr.com***.