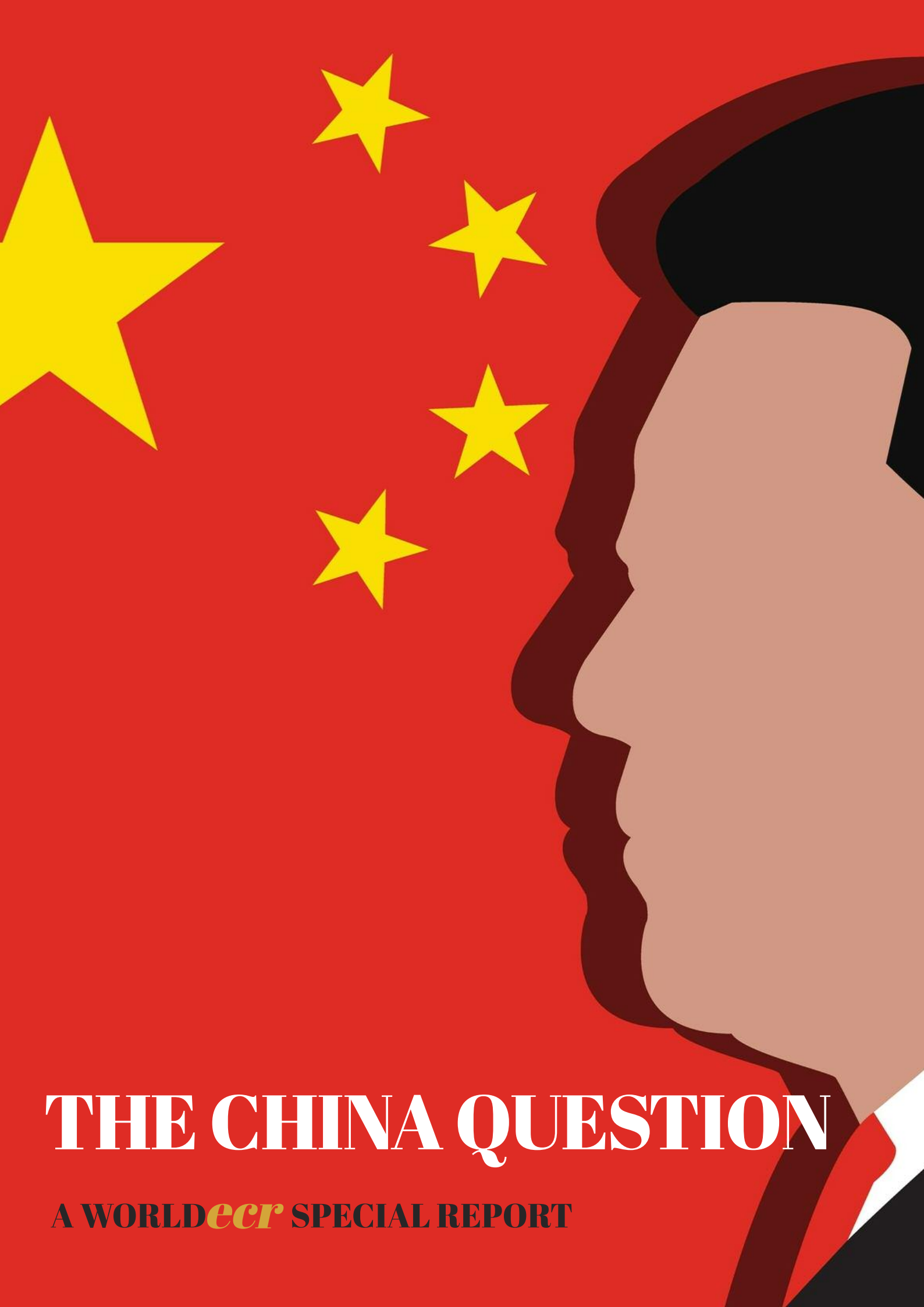
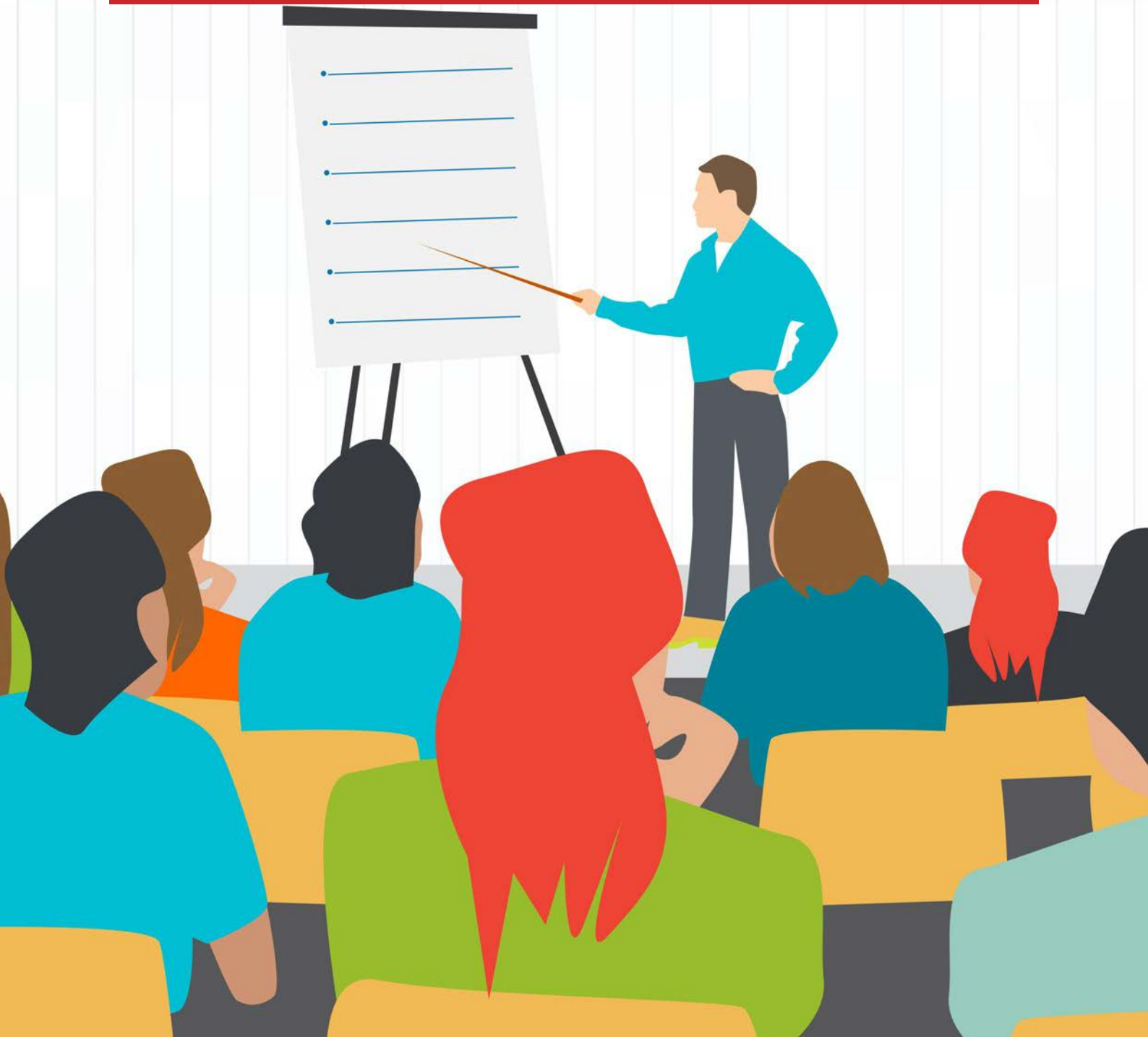


THE CHINA QUESTION

A WORLD*ecr* SPECIAL REPORT



Growing pressure on US universities to police against Chinese influence

By David A. Ring and Tahlia Townsend, Wiggin and Dana

Perhaps it would be an understatement to say that it has been an interesting few years for those responsible for maintaining university compliance programmes. Of course, there has been the ordinary, but always challenging, trade compliance task of making sure that each item exported by the university is properly classified and authorised for export; a problem Princeton recently experienced first-hand when it was fined $54,000 and required to undergo an external audit, as a result of its failure to obtain licences for pathogens that were controlled for chemical and biological weapons reasons. But a significant new set of challenges has arisen from the United States' whole-of-government approach to countering the perceived threat from China, which has resulted in a plethora of new compliance obligations stemming from multiple government sources, many developed without the benefit of standard notice-and-comment rulemaking and requiring rapid implementation.

While it is beyond the scope of this article to survey every China-related compliance obligation that has developed over the past few years, the following sample shows the diversity and depth of the new requirements and enforcement trends:

- Section 889 of the National Defense Authorization Act of 2019 was extended to grant recipients via 2 C.F.R. 200.216, thereby prohibiting universities from using grant money to procure telecommunications equipment, or services or systems that use equipment, produced by Huawei, ZTE, and certain other Chinese telecom manufacturers;
- The Department of Commerce, Bureau of Industry and Security ('BIS') amended 15 C.F.R. 744.21 to extend the prohibition on exporting certain items for military end-use in China to encompass exports to military end-users in China, a term that is broadly defined to include any party that supports or contributes to the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of 'military items', and that potentially reaches many Chinese commercial, academic, and research entities. While BIS ultimately published a list of identified Chinese military end-users, that list is by no means exhaustive, and compliance personnel are still left to determine, through independent due diligence, whether any given Chinese institution is involved in activities that could cause it to be considered a 'military end-user';
- BIS also added a new rule at 15 C.F.R. § 744.22 and revised existing 15 C.F.R. § 744.6 to (i) impose a licence requirement on exports/reexports/transfers of any item subject to the EAR (including EAR99 items) to a 'military-intelligence end-use' or a 'military-intelligence end-user' in China (or Cuba, Iran, Syria, North Korea, Burma, Russia, or Venezuela), and (ii) absent a licence, prohibit US persons from engaging in any activity that 'may assist or benefit' military-intelligence end-users or end-uses in those countries, whether or not the activities involve items that are subject to the EAR. Because the rule applies even to activities involving no items subject to the EAR, universities must undertake due diligence to determine whether proposed activity by university personnel could 'assist or benefit' any intelligence or reconnaissance organisation of the PRC armed services or national guard (including but certainly not limited to the many-tentacled Intelligence Bureau of the Joint Staff Department) even with respect to projects, travel, and guest lectures that exclusively involve 'published' materials or 'fundamental research', and that would therefore typically be exempt from US export controls; and
- BIS has added numerous Chinese universities, research centres and technical institutes to the Entity List, thus further compelling universities to screen its Chinese partners and any party that might be considered an end-user of the products or technology to be exported.

A significant new set of challenges has arisen from the United States' whole-of-government approach to countering the perceived threat from China, which has resulted in a plethora of new compliance obligations.

Academics in the spotlight

Beyond the implementation of entirely new rules, there have been the highly publicised criminal prosecutions of professors and visiting scholars under a variety of existing authorities, with charges ranging from defrauding federal agencies by failing to disclose Chinese affiliations in grant applications, to espionage, visa fraud, failure to file as a foreign agent, theft of intellectual property, and tax fraud. While

these prosecutions, to date, have focused solely on individuals, they have had a clear impact on universities, which must adapt to the underlying evolution of grant agencies' interpretations of their rules for disclosing Chinese affiliations, and which have been left to decide whether relying on grant applicants' self-disclosure of conflicts is sufficient to protect against criminal prosecution.

The change of US administrations in January 2021 has done little to dampen the enthusiasm for new laws and rules intended to prevent universities from sharing technology with China. Despite a petition from academia urging reconsideration, the Biden administration has indicated that it will retain President Trump's National Security Presidential Memorandum-33 ('NSPM-33'), which greatly expands disclosure requirements for parties applying for funding or participating in certain activities within 'the federal research enterprise', across all government agencies. Together with a report issued by the National Science and Technology Council's Joint Committee on the Research Environment ('the JCORE Report'), NSPM-33 provides a long list of required and 'recommended' disclosures and compliance practices for research institutions, intended to identify foreign influence over not only principal investigators but also 'other senior/key personnel' on federal grants, agency programme officers, peer reviewers, and advisory committee members. (Indeed, the JCORE Report goes even further, recommending collection of disclosure information even from postdocs and from visiting scholars and graduate students participating in relevant research activities.) The implication of these documents is clear: universities need to do more to police their own and to collaborate with US law enforcement.

Moreover, additional changes may soon come from the Innovation and Competition Act of 2021 ('the Act'), which was recently passed by the Senate with bi-partisan support. While the Act appears to walk back proposals to require certain foreign gifts and contracts to undergo review by the Committee on Foreign Investment in the United States ('CFIUS'), there are a number of other provisions relevant to university compliance. For instance, Section 2303 would outright prohibit federal grants to projects led or supported by researchers who participate in a Chinese (or Russian, North Korean, or Iranian) foreign government talent recruitment programme, such as the now-notorious 'Thousand Talents' programme. Likewise, expanding on Department of Defense funding restrictions passed in 2019 as part of the National Defense Authorization Act, Section 2525 would prohibit National Science Foundation grants to, and Section 6122 would impose compliance conditions on receipt of most Higher Education Act funds by, universities that host or support Confucius Institutes.

More significantly, Section 4494 would make it a crime for an individual to 'knowingly prepare or submit' a federal grant application that fails to disclose receipt of outside compensation, including foreign compensation (defined as 'a title, monetary compensation, access to a laboratory or other resource, or other benefit received from – (A) a foreign government; (B) a foreign government institution; or (C) a foreign public enterprise'). This provision will make criminal enforcement of individuals substantially easier by alleviating the government's current burden to show that failures to disclose such compensation were part of a scheme to defraud the government or university.

Section 4497 would require J-1 'visiting scholar' visa sponsors to certify: (i) that they comply with export regulations; (ii) that export licences are not required for technology that will be accessed by the visa applicant; (iii) that they will prevent access to controlled technology by the visa applicant; and (iv) that they will submit a technology control plan showing how they intend to comply. And Section 6124 would lower the reporting threshold under Section 117 of the Higher Education Act ('HEA') for gifts and contracts from foreign sources from $250,000 to $50,000, and authorise fines for non-disclosure of between $250 and the value of the gift or contract (or up to $100,000 or twice the value of the gift or contract in the case of wilful failure to disclose for three consecutive years).

These rules and proposals point to the likelihood that universities will be compelled to take a more proactive – if not outright investigatory – approach to China-related compliance obligations.

Section 6124 would also add a new provision to the HEA requiring universities with more than $5 million in annual research expenditures to set up a searchable database of foreign gifts and contracts received by research faculty and staff and to 'maintain a plan to effectively identify and manage potential information gathering by foreign sources through espionage targeting faculty, professional staff, and other staff engaged in research and development … that may arise from gifts received from, or contracts entered into with, a foreign source.'

All of these rules and proposals point to the likelihood that universities will be compelled to take a more proactive – if not outright investigatory – approach to China-related compliance obligations, including significant efforts to ensure that researchers and other personnel are not supported or influenced by China or its institutions. □

David A. Ring (dring@wiggin.com) is a partner at Wiggin and Dana where he represents US and non-US clients in matters relating to US export controls and sanctions. He has served as a US State Department-appointed monitor, and provides counsel and training to some of the world's largest aerospace and defence companies.

Tahlia Townsend (ttownsend@wiggin.com) is a partner and Co-chair of the International Trade Compliance practice at Wiggin and Dana. Tahlia advises companies on, and defends companies in enforcement actions involving, US financial sanctions, export controls, and US foreign investment regulations.

A WORLD*ecr* SPECIAL REPORT

WorldECR is published by D.C. Houghton – the world's leading specialist publisher of trade compliance publications.

D.C. Houghton produces:

COMPLIANCE JOURNALS: Export Compliance Manager and FISC - Financial Institutions Sanctions Compliance; WorldECR, the journal of export controls and sanctions

BEST-SELLING BOOKS: Export Compliance Manager's Handbook; Sanctions in Europe; World Encryption Controls; Dual-use Export Controls in International Transit and Transhipment; Dual-use Export Controls of the European Union; Asia Pacific Strategic Trade Controls; The CFIUS Book

COMPLIANCE CONFERENCES AND WEBINARS AND TRAINING

BESPOKE RESEARCH PUBLISHING

Please visit our websites worldecr.com and exportcompliancemanager.com for more information.