LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# US' New China Tech Unit Raises Domestic Research Scrutiny

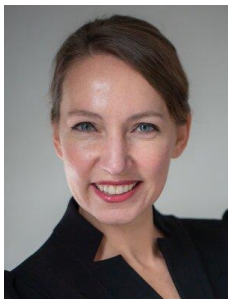
By **Michael Atkinson, Caroline Brown and Jeremy Iloulian**
(March 17, 2023, 5:05 PM EDT)

Last month, the U.S. Department of Justice and U.S. Department of Commerce announced a new Disruptive Technology Strike Force.

Michael Atkinson

The strike force will bring together experts throughout government — including the FBI, Homeland Security Investigations and 14 U.S. attorneys' offices in 12 metropolitan regions across the country — to target illicit actors, strengthen supply chains, and protect critical technological assets from being acquired or used by nation-state adversaries.

The strike force will be co-led by DOJ's National Security Division and the Commerce Department's Bureau of Industry and Security.



Caroline Brown

Though four countries are named as nation-state adversaries, the underlying theme and focus is China, which has been the main rival of the U.S. government in the contest for technological leadership. The other three named countries — Iran, North Korea and Russia — are already subject to significant U.S. sanctions and export restrictions.

Critical to technological supremacy is unfettered access to advanced technologies and their human talent, the protection of which is the rationale underlying the increasing number of critical technology trade controls and the Disruptive Technology Strike Force.

Jeremy Iloulian

While the strike force itself does not create any new authority for the U.S. government, it further buttresses existing technology and China-focused controls by holding accountable those that unlawfully acquire critical technology in violation of these controls. Included in that suite of controls are the prohibitions imposed on private sector research institutions and U.S. universities and higher education institutions related to China.

These prohibitions manifest themselves in the regulations of an array of U.S. government entities, including the Department of Commerce, U.S. Department of Defense, U.S. Department of Education and U.S. Department of Energy, as well as NASA, the National Institutes of Health and the National Science Foundation.

Though some of the restrictions only apply upon receipt of U.S. government financial support or contracts, others — such as U.S. export controls — are broader.

Private sector research institutions, government contractors, and U.S. universities and research facilities, in particular, should ensure that they are aware of, and in compliance with, existing prohibitions and continue to monitor for new ones.

Many times, the most efficient compliance program is one that is broad enough to incorporate each of the specific components.

**View From Washington**

The Disruptive Technology Strike Force aligns with the DOJ's transition away from its China Initiative to a broader strategy to counter nation-state threats.

The China Initiative, which the DOJ established in 2018 to develop a coherent approach to the national security challenges posed by the People's Republic of China, was criticized by the civil rights community for fueling a narrative of bias and concerns from the academic and scientific community, in particular, for unfairly targeting people from China or of Chinese descent for their alleged ties to the Chinese government.

In response, the leader of DOJ's National Security Division, Assistant Attorney General Matthew Olsen, announced in public remarks one year ago the end of the China Initiative and its replacement by a new strategy for countering nation-state threats.[1]

Consistent with that new strategy, the Disruptive Technology Strike Force aims to counter the same nation-state threats previously identified, namely, China, Russia, Iran and North Korea, but without naming one specific country.

The strike force also seeks to advance two strategic imperatives identified by Olsen on the one-year anniversary of his public remarks: defending the U.S. from threats of export controls evasion and protecting key technologies. Along these lines, the strike force will focus on, among other things, investigating and prosecuting criminal violations of export laws, and enhancing administrative enforcement of U.S. export controls.

The press release announcing the Disruptive Technology Strike Force also highlighted the importance of advanced technologies, which include supercomputing and exascale computing, artificial intelligence, advanced manufacturing equipment and materials, quantum computing, and biosciences.

Although the name of the DOJ's new nation-state strategy no longer focuses exclusively on China — in an effort to mitigate the narrative of bias — the U.S. has declared that China is "the most serious long-term challenge to the international order," particularly when it comes to advanced technologies.[2]

These advanced technologies, like supercomputing and artificial intelligence, sit at an intersection between commercial and military uses, and will require continued and constant clear-eyed vigilance for those on the front lines of this technological competition, especially U.S. universities and research facilities.

**The National Security Legal Regimes Applicable to Universities and Research Facilities**

To protect U.S. technological and scientific advantages, the U.S. has developed legal architecture to impose requirements and restrictions on private sector research institutions, government contractors and U.S. higher education institutions.

However, unlike other legal regimes, there is no single U.S. agency responsible for the implementation of rules guarding against the unlawful acquisition or theft of technology.

The White House has issued some centralizing guidance in the form of National Security Presidential Memorandum 33, which requires research agencies to collect certain foreign disclosures from their applicants, but a number of agencies implement their own distinct regulations, making funding grants contingent upon compliance with those regulations.

The table below summarizes some of the restrictions. Note that each is a summary only and does not capture exceptions or carveouts that may apply.

| U.S. AGENCY | RESTRICTIONS APPLICABLE TO RESEARCH INSTITUTIONS & UNIVERSITIES |
|---|---|
| BIS | Deemed Export Risks (15 C.F.R. § 734.15))<br>Providing software or technology to non-U.S. nationals or green card holders (e.g., visiting professors) can constitute an export and require an export license. |
| | Academic Outreach Initiative<br>Announced in June 2022, BIS will prioritize select institutions depending on whether the institution maintains any foreign partnerships with export-restricted parties, engages in DOD-related research, or researches "sensitive" technologies. Commerce will send "outreach agents" to help establish partnerships with universities and provide briefings and trainings. |
| U.S. Department of Defense ("DOD") | Memo on Protecting IP, Controlled Info, Key Persons, Critical Technology (DFARS Case 2021-D023)<br>DOD is required to ask each individual working on a DOD grant funded project to disclose current and historic research, and their funding sources per a March 2019 memorandum. |
| | Funding Restrictions for Hosting Confucius Institutes (DFARS Case 2021-D023)<br>Would prohibit DOD from awarding any contracts to institutions that host a Confucius Institute (not yet implemented). DOD noted that a report on this topic will be issued in March 2023 |
| U.S. Department of Education | Disclosure Report for Section 117 of the Higher Education Act (20 U.S.C. § 1011f(a))<br>Section 117 requires an "institution" to file a disclosure report when it "receives a gift from or enters into a contract with a foreign source" that is – alone or in aggregate within the calendar year from the same foreign source – valued at $250,000 or more. |
| U.S. Department of Energy ("DOE") | Foreign Talent Prohibition (DOE Order 486.1a)<br>DOE federal and contractor employees are (i) prohibited from participating in certain foreign government talent recruitment programs; and (ii) expected to engage in certain due diligence requirements to confirm they are in compliance. The initial order was issued in 2019, but was updated in 2020. |
| NASA | Chinese Funding Prohibition (Pub. L. 117-103 (Sec. 526))<br>Since 2011, NASA has annually been prohibited from funding any work involving China or any Chinese-owned company. Therefore, proposals for grants cannot include bilateral participation, collaboration, or coordination with any such entity, as they would ineligible. |
| National Institutes of Health ("NIH") | Reminder of NIH Policies on Conflicts of Interest and Foreign Components (NOT-OD-19-114)<br>NIH applicants are required to list all foreign appointments, foreign support, current projects supported by foreign entities, and participation in foreign talent programs per a July 2019 notice. |
| National Science Foundation ("NSF") | Letter on Prohibiting Participation in Foreign Talent Programs (NSF-19-200)<br>NSF personnel and intergovernmental personnel assignment act persons detailed to NSF are prohibited from participating in foreign government talent recruitment programs per a letter from July 2019. |
| | Foreign Funding Disclosure Requirements<br>NSF requires senior project personnel to disclose all foreign (and domestic) support for proposals, a requirement which was updated and clarified in 2019-2020. |

**Examples of Recent University-Related Enforcement Actions**

Since the Biden administration's inauguration, the DOJ has investigated and prosecuted a number of universities, even after terminating its China Initiative.

DOJ officials have explained in these cases that "failing to comply with federal disclosure obligations is not tolerable. Period," and that the DOJ will hold accountable all "institutions, agencies, and researchers."[3]

***The Ohio State University***

In November 2022, the DOJ issued a press release that The Ohio State University paid a $875,689 settlement to resolve civil allegations that it failed to disclose that an unidentified OSU professor received support from a foreign government in breach of the grant and research provisions related to the U.S. Army, NASA and NSF.[4]

In May 2021 OSU professor Song Guo Zheng, was sentenced to 37 months in prison and ordered to pay approximately $3.8 million in fees to the NIH and OSU due to false statements to federal authorities as part of an immunology research fraud scheme.[9]

This professor lied about his participation in China's Thousand Talents program and providing research to China.

***Texas A&M University***

In September 2022, Zhengdong Cheng, a former Texas A&M University professor pleaded guilty to violating NASA regulations restricting work with China and falsifying official documents after receiving almost $750,000 in grants for space research.[5] He agreed to pay restitution of $86,876 and a fine of $20,000.

***University of Arkansas***

In June 2022, a former University of Arkansas professor, Simon Saw-Teong Ang, was sentenced to just over one year in prison for making a false statement to the FBI about the existence of patents for his inventions in China.[6]

Despite listing himself as the inventor for 24 patents in China, the former professor failed to disclose this to his university and denied his involvement when questioned by the FBI.

***University of Kansas***

In April 2022, a U.S. District Court for the District of Kansas jury convicted former University of Kansas professor Feng Tao of wire fraud and making false statements in concealing his appointment at Fuzhou University in China, while participating in DOE- and NSF-funded projects.[7]

While U.S. District Judge Julie Robinson later ruled there was insufficient evidence to support the wire fraud counts, she upheld the false statement charge and sentenced the professor to time served and two years of supervised release, without a fine or restitution.[8]

**Examples of Private Sector Risks**

In addition to the risks that universities face, recent law enforcement actions have also highlighted threats to public companies and government contractors engaging in their own research programs. These research facilities, particularly those engaging in critical, emerging or defense technologies, are a target for foreign intelligence programs. Below are some examples from this January.

***Espionage Recruitment***

Last September, a U.S. District Court for the Northern District of Illinois jury found Chinese national Ji Chaoqun guilty for acting illegally within the U.S. as an agent of China, specifically at the direction of high-level Chinese intelligence officers to identify engineers and scientists at U.S. defense contractors for possible recruitment. In January, Chaoqun was sentenced to eight years in prison.[10]

Last year, Chaoqun's supervisor, Yanjun Xu, was sentenced to 20 years in federal prison after himself being convicted of conspiracy and attempting to commit economic espionage and theft of trade secrets.[11]

***Export Controls Violation***

In January, Jonathan Yet Wing Soong, a former employee of NASA contractor Universities Space Research Association, pleaded guilty to violating export control laws in a scheme to use an intermediary buyer to sell flight control software, used by the U.S. Army, to Beihang University in China, a party on the Department of Commerce's entity list.[12]

***Foreign Talent Program***

Also in January, the U.S. District Court for the Northern District of New York sentenced Xiaoqing Zheng, a former General Electric engineer and a member of China's Thousand Talents Program, to two years in prison and a $7,500 fine for conspiring to steal information about the company's turbine technology on behalf of Chinese state entities.[13]

**Actions Taken by Other Countries**

The U.S. is not the only jurisdiction concerned about these types of issues, and other countries have begun to act. For example, last month Japan and the Netherlands reportedly[14] agreed to tighten restrictions on the export of chip manufacturing technology to Chinese companies, which was immediately followed by a report that a Chinese employee of a key Dutch chip equipment manufacturer stole data from the company.[15]

The year prior, Dutch university Vrije Universiteit began returning funds to a Chinese university donor after an investigation by the Dutch press identified that the university promoted positions similar to the Chinese government.[16]

Additionally, in May 2022, Japan began asking its universities to enhance screening of foreign visitors to prevent technological theft.[17]

The United Kingdom outright prohibited a licensing deal in July 2022 where the University of Manchester would license sensors to a Chinese entity.[18]

**What's Next**

The passage of the Creating Helpful Incentives to Produce Semiconductors and Science, or CHIPS+, Act, will now usher in a new set of foreign talent program requirements. The CHIPS+ Act, known for its support of domestic semiconductor and critical technology development, also includes a provision that broadly prohibits federal employees, contractors and awardees from participating in foreign talent programs, taking it one step further than National Security Presidential Memorandum 33, which only requires disclosure of those programs.

Finally, Congress has pushed, and will likely continue to push, other bills targeting perceived risks associated with universities and research institutions. One example is a bill that would prohibit federal funding for universities if they employ a Chinese Communist Party-funded instructor, while another would require the mandatory disclosure of any donation over $5,000 from a Chinese-affiliated entity.[19]

These bills did not advance in the prior Congress, but given the anti-China sentiment on both sides of the aisle, it is possible actions like this could gain traction.

**Key Takeaways**

The potential repercussions for noncompliance with U.S. export controls, government funding restrictions and other similar China controls will increase with the development of the Disruptive Technology Strike Force.

Universities should use a formalized information collection program to ensure full awareness of who their researchers, professors and other staff members are partnering with, even in the context of work unrelated to the university.

All non-U.S. partnerships should be monitored, especially if any involve Chinese or Russian entities, in the event that the partnering entity becomes subject to U.S., EU, U.K. or other economic sanctions or export restrictions.

Leadership should effectively communicate the risks associated with these types of partnerships and support strong compliance programs, training and the creation of whistleblower hotlines for employees, researchers and staff.

Day-to-day monitoring of researchers to ensure continued compliance with any grant provisions is equally critical to limit any violations to minor infractions, and avoid any acceleration of issues.

Private sector research institutions, government contractors and universities should be prepared for a future where all dealings with China — and Russia — particularly those involving advanced technologies, will become subject to heightened scrutiny.

---

*Michael Atkinson is a partner and the co-leader of the national security practice at Crowell & Moring LLP. He previously served two decades in various senior roles at the DOJ, including acting deputy assistant attorney general of the National Security Division and U.S. intelligence community inspector general.*

*Caroline Brown is a partner and the co-leader of the national security practice at the firm. She previously served over a decade in various roles at the DOJ's National Security Division and at the U.S. Department of the Treasury.*

*Jeremy Iloulian is an associate at the firm.*

*Kelsey Clinton, an associate at the firm, contributed to this article.*



[1] Assistant Attorney General Matthew Olsen, Remarks on Countering Naitno-State Threats (Feb. 23, 2022), https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-olsen-delivers-remarks-countering-nation-state-threats.

[2] Antony J, Blinken, Secretary of State, Speech on the Administration's Approach to the People's Republic of China (May 26, 2022), https://www.state.gov/the-administrations-approach-to-the-peoples-republic-of-china/.

[3] Ohio State University Pays Over $875,000 to Resolve Allegations that It Failed to Disclose Professor's Foreign Government Support (Nov. 10, 2022), https://www.justice.gov/opa/pr/ohio-state-university-pays-over-875000-resolve-allegations-it-failed-disclose-professor-s.

[4] Ohio State University Pays Over $875,000 to Resolve Allegations that It Failed to Disclose Professor's Foreign Government Support (Nov. 10, 2022), https://www.justice.gov/opa/pr/ohio-state-university-pays-over-875000-resolve-allegations-it-failed-disclose-professor-s.

[5] Juan A. Lozano, Professor, NASA Researcher Pleads Guilty in China Ties Case (Sept. 23, 2022), https://apnews.com/article/china-texas-houston-b1ffd9c4dd96f8328886febf16d002c2.

[6] Former University of Arkansas Professor Sentenced to a Year and a Day for Lying to Federal Agents About Patents in China (June 16, 2022), https://www.justice.gov/opa/pr/former-university-arkansas-professor-sentenced-year-and-day-lying-federal-agents-about.

[7] Jury Convicts University of Kansas Researcher for Hiding Ties to Chinese Government (Apr. 7, 2022), https://www.justice.gov/opa/pr/jury-convicts-university-kansas-researcher-hiding-ties-chinese-government.

[8] Margaret Stafford, Kansas Researcher Given Time Served in China-related Case (Jan. 18, 2023), https://apnews.com/article/legal-proceedings-kansas-city-china-education-bb13875a7debdfef0b3184f04b9ec9b5.

[9] University Researcher Sentenced to Prison for Lying on Grant Applications to Develop Scientific Expertise for China (May 14, 2021), https://www.justice.gov/opa/pr/university-researcher-sentenced-prison-lying-grant-applications-develop-scientific-expertise.

[10] Chinese National Sentenced to Eight Years for Acting within the United States as an Unregistered Agent of the People's Republic of China (Jan. 25, 2023), https://www.justice.gov/opa/pr/chinese-

national-sentenced-eight-years-acting-within-united-states-unregistered-agent-people.

[11] Chinese Government Intelligence Officer Sentenced to 20 Years in Prison for Espionage Crimes, Attempting to Steal Trade Secrets from Cincinnati Company (Nov. 16, 2022), https://www.justice.gov/usao-sdoh/pr/chinese-government-intelligence-officer-sentenced-20-years-prison-espionage-crimes.

[12] Castro Valley Resident Pleads Guilty to Illegally Exporting American Aviation Technology to Beijing University (Jan. 17, 2023), https://www.justice.gov/usao-ndca/pr/castro-valley-resident-pleads-guilty-illegally-exporting-american-aviation-technology.

[13] Former GE Power Engineer Sentenced for Conspiracy to Commit Economic Espionage (Jan. 3, 2023), https://www.justice.gov/opa/pr/former-ge-power-engineer-sentenced-conspiracy-commit-economic-espionage.

[14] Jenny Leonard and Cagan Koc, Biden Nears Win as Japan, Dutch Back China Chip Controls (Jan. 26, 2023), https://www.bloomberg.com/news/articles/2023-01-27/japan-netherlands-to-join-us-in-chip-export-controls-on-china?sref=ExbtjcSG#xj4y7vzkg.

[15] Annabella Liang, US-China Chip War: ASML Says China Employee Stole Data (Feb. 16, 2023), https://www.bbc.com/news/business-64658843.

[16] Jon Henley, Dutch University Gives Up Chinese Funding Due to Impartiality Concerns, (Jan. 25, 2022), https://www.theguardian.com/world/2022/jan/25/dutch-university-gives-up-chinese-funding-due-to-impartiality-concerns.

[17] Ju-min Park, With Eye on China, and U.S. Ties, Japan's Universities to Screen Foreigners (May 23, 2022), https://www.reuters.com/world/asia-pacific/with-eye-china-us-ties-japans-universities-screen-foreigners-2022-05-23/.

[18] National Security and Investment Act, Notice of Final Order (July 20, 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092802/aquisition-scamp5-scamp7-know-how-final-order-notice-20220720.pdf.

[19] The prohibition bill is H.R. 2258 – Protecting Higher Education from Foreign Threats Act. See https://www.congress.gov/bill/117th-congress/house-bill/2258/text?r=10&s=1. While the mandatory disclosure bill is the Preventing Malign Chinese Influence on Academic Institutions Act. See https://www.kennedy.senate.gov/public/press-releases?ID=E10BC6A3-6D40-4755-933B-9CA2253DEC2F.