Statement before the
Senate Committee on Banking, Housing, and Urban Affairs
"CFIUS Reform: Examining the Essential Elements,"

A Testimony by:

James Mulvenon, Ph.D.
General Manager, Special Programs Division
SOS International

January 18, 2018

538 Dirksen Senate Office Building

Introduction and Main Points

Chairman Crapo, Ranking Member Brown, and distinguished members, thank you for inviting me to testify today.

In 2013, two U.S. government colleagues and I published a book entitled *Chinese Industrial Espionage*, which documented the efforts, both quasi-legal and illegal, used by the Chinese government and state-owned entities to steal U.S. technology, intellectual property, and secrets.[1] For me, this culminated almost two decades of tracking Chinese cyber espionage and the PRC military and defense industrial base's efforts at illicit technology transfer.

The current main problem as I see it is two-fold. One, the Chinese government has a comprehensive strategy for national economic growth and technology modernization. This strategy has created an unfair, asymmetric business environment in China, sometimes forcing American companies, who need to be in the China market to grow and prosper, to make suboptimal decisions that are not always in the long-term interests of U.S. national security, but clearly benefit Chinese national security. Two, U.S. laws and regulations governing Chinese investment in the United States, U.S. company technology transfers, and export controls have not evolved sufficiently to deal with Beijing's aggressive and constantly evolving strategy. In fact, early successes in the Committee for Foreign Investment in the United States (CFIUS) process in preventing inappropriate acquisition deals, such as the rejection of the Huawei-3COM deal, led Beijing to conclude that overt acquisition efforts, while preferred, would not always succeed, and led Chinese entities to adapt from outright acquisition to joint ventures and other investment vehicles typically outside the current CFIUS scope, using the power of access to the China market to leverage technology transfer. For example, Tsinghua Unigroup's attempted but failed minority investment into U.S. hard drive maker Western Digital is another case where Beijing had attempted to end-run CFIUS with creative investment structures,[2] as was the failed attempt by Canyon Bridge, an acquisition proxy of the Chinese State Council, to purchase Lattice Semiconductor.[3] These are the examples where CFIUS worked, and yet unfortunately, the number of examples where China has successfully avoided U.S. regulatory regimes to prevent technology transfer harmful U.S. national security are increasing. The Chinese are learning our system, identifying its gaps and weaknesses, and finding new ways to exploit American technology to their advantage.

More importantly, these activities have a direct and lasting negative impact on U.S. national security. As the Communist Party seeks to enhance all aspects of its national comprehensive

---

[1] William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, London: Routledge, May 2013.
[2] Joshua Jamerson and Eva Dou, "Chinese Firm Ends Investment in Western Digital, Complicating SanDisk Tie-Up," *Wall Street Journal*, 23 February 2016, accessed at: https://www.wsj.com/articles/unispledour-ends-investment-in-western-digital-complicating-sandisk-tie-up-1456231018
[3] Liana Baker, "Trump Bars Chinese-Backed Firm from Buying U.S. Chipmaker Lattice," *Reuters*, 13 September 2017, https://www.reuters.com/article/us-lattice-m-a-canyonbridge-trump/trump-bars-chinese-backed-firm-from-buying-u-s-chipmaker-lattice-idUSKCN1BO2ME

power, U.S. comparative advantages will become all the more important in sustaining U.S. leadership on the battlefield, including in advanced technologies. For example, the Pentagon's "third offset" strategy seeks to leverage current U.S. commercial technological advantages in key areas, such as artificial intelligence and machine learning, to enhance our war fighting capability vis-a-vis China and a resurgent Russia.[4] Yet if our porous investment security and export control regime is not improved, Beijing may be able to turn these current American advantages into their own by investing in, acquiring, or co-opting critical technology. This will allow China to deny the United States' ability to leverage critical technologies for its national security, and further close the gap with the U.S. in areas of key military systems and applications ranging from hypersonic glide vehicles to AI-enabled cyber defense systems.

Although American companies are one of Beijing's highest priority targets in the race to close the technological gap with the United States, the current tech transfer crisis is not entirely their fault. In the China market, American companies confront a comprehensive, state-directed economic and technology development strategy designed to promote technology transfer from foreign multinationals and elevate domestic companies to compete with those multinationals in the global market.[5] This strategy is one personally touted by President Xi Jinping, who declared at a recent Communist Party Meeting that the Chinese state must determine which technologies to develop on its own, which to induce or co-opt from abroad, and which to develop in partnership with Chinese entities.[6] Xi's personal vision has been codified into a more concrete strategy with a number of key overt features:

- Promulgation of state industrial planning documents outlining how Beijing would use its substantial regulatory leverage and financial resources to promote technology transfer and (e.g., "2006-2020 Mid-to-Long Range S&T Plan" and "Made in China 2025"[7])
- Implementation of the strategy of "military-civilian fusion" that expands "civil-military integration" of defense and civilian industrial bases to facilitate the "construction of a national infrastructure that connects the PLA, state-owned defense research, development, and manufacturing enterprises, government agencies under the State Council, universities, and private sector firms."[8]

---

[4] https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/

[5] For an overview, see Jane Perlez, Paul Mozur And Jonathan Ansfield, "China's Technology Ambitions Could Upset the Global Trade Order," *New York Times*, 7 November 2017, accessed at:
https://www.nytimes.com/2017/11/07/business/made-in-china-technology-trade.html?_r=0

[6] https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/

[7] See U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, accessed at:
https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

[8] Greg Levesque and Mark Stokes, *Blurred Lines: Military-Civil Fusion and the "Going Out" of China's Defense Industry*, Pointe Bello, December 2016, accessed at:
https://static1.squarespace.com/static/569925bfe0327c837e2e9a94/t/593dad0320099e64e1ca92a5/1497214574912/062017_Pointe+Bello_Military+Civil+Fusion+Report.pdf

- Provision of massive state subsidies (e.g., IC Fund) to benefit Chinese companies, often masked in ways to skirt WTO prohibitions (according to the U.S Chamber's analysis of Made in China 2025, China will "provide preferential access to capital to domestic companies in order to promote their indigenous research and development capabilities, *support their ability to acquire technology from abroad*, and enhance their overall competitiveness"[9]). Other benefits include "fiscal stimulus, tax reductions and holidays, access to low-cost or free land, low-interest credit, easier access to securities markets, patent approvals, discriminatory technical standards, antitrust policy directed against disfavored competitors, privileged government procurement, limits on market access, and other preferential policies."[10]
- Promotion of "national champion" companies (e.g., Huawei) to supplant multinational companies in the China market and globally[11]
- Promulgation of laws and regulations codifying asymmetries in playing field for U.S. companies operating in China using a very broad definition for what constitutes national security (e.g., Anti-Monopoly Law,[12] Cybersecurity Law,[13] Counter-Espionage Law,[14] National Security Law,[15] Counter-Terrorism Law[16])
- The use of a domestic standards regime, especially with respect to information communication and telecommunications, as a trade weapon to advantage Chinese companies (e.g., WAPI, draft China CPU/OS/computer standards, and the 5G cellular standard)[17]

---

[9] See U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, accessed at: https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

[10] Scott Kennedy, "Evaluating CFIUS: Challenges Posed by a Changing Global Economy," Statement Before the House Committee on Financial Services, Subcommittee on Monetary Policy and Trade, 9 January 2018, accessed at: https://financialservices.house.gov/uploadedfiles/hhrg-115-ba19-wstate-skennedy-20180109.pdf

[11] James McGregor, *China's Drive for 'Indigenous Innovation: A Web of Industrial Policies*, Washington, DC: US Chamber of Commerce, July 2010.

[12] U.S. Chamber of Commerce, *Competing Interests in China's Competition Law Enforcement: China's Anti-Monopoly Law Application and the Role of Industrial Policy*, accessed at: https://www.uschamber.com/sites/default/files/aml_final_090814_final_locked.pdf

[13] https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en

[14] https://www.chinalawtranslate.com/anti-espionage/?lang=en

[15] http://www.chinalawtranslate.com/2015nsl/?lang=en

[16] https://www.chinalawtranslate.com/%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95-%EF%BC%882015%EF%BC%89/?lang=en

[17] Dan Breznitz and Michael Murphree, "The Rise of China in Technology Standards: New Norms in Old Institutions," report prepared for the U.S.-China Economic and Security Review Commission, 16 January 2013, accessed at: https://www.uscc.gov/sites/default/files/Research/RiseofChinainTechnologyStandards.pdf

- Promotion of "buy local" laws to disadvantage foreign firms, especially in information and communications technologies[18]
- Strategies to attract priority foreign investment in China, especially joint ventures and "greenfield" investments[19]
- Mercantilist investment structures globally designed to create infrastructure path dependencies for Chinese state-owned enterprises ("One Belt, One Road")[20] and quasi private companies that China aims to ensure will provide the hardware and software that will underpin all critical infrastructure of the future, from power grids to telecom networks to e-payments infrastructure.

And some covert, illicit features:

- Beijing's well-documented, planetary-scale, government-directed cyber espionage program[21]
- Large-scale, government-directed technology espionage[22]

---

[18] U.S. Chamber of Commerce, *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT*, 2016, accessed at: https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf

[19] For the best data on the subject, see the American Enterprise Institute's China Global Investment Tracker at https://www.aei.org/china-global-investment-tracker/ and The Rhodium Group's China Investment Monitor at http://rhg.com/interactive/china-investment-monitor

[20] Christopher Johnson, *President Xi Jinping's "Belt and Road" Initiative: A Practical Assessment of the Chinese Communist Party's Roadmap for China's Global Resurgence,* Center for Strategic and International Studies, March 2016, accessed at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160328_Johnson_PresidentXiJinping_Web.pdf

[21] See *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, Office of the National Counterintelligence Executive, October 2011, at https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; ThreatConnect, *CameraShy: Closing the Aperture on China's Unit 78020*, at https://www.threatconnect.com/camerashy/; Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; Dmitri Alperovitch, *Revealed: Operation Shady RAT*, McAfee, August 2011; McAfee® Foundstone® Professional Services and McAfee Labs, Global Energy Cyberattacks: 'Night Dragon', 10 February 2011, accessed at: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf; Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, (report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp), March 7, 2012; and *Operation SMN: Axiom Threat Actor Group Report*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[22] Peter Mattis, "Testimony before the U.S.-China Economic and Security Review Commission: Chinese Human Intelligence Operations against the United States," 2 June 2016,

- Non-traditional collection (e.g., the "1000 Talents Program")[23]
- New types of hybrid cyber and human technology espionage (According to the 2016 U.S-China Economic and Security Review Commission report: "China appears to be conducting a campaign of commercial espionage against U.S. companies involving a combination of cyber espionage and human infiltration to systematically penetrate the information systems of U.S. companies to steal their intellectual property, devalue them, and acquire them at dramatically reduced prices."[24])

Any one of these strategies or policies in isolation would be problematic for the U.S. government and American companies, but their simultaneous and often coordinated implementation with the explicit support of PRC government leadership presents an unprecedented challenge.

Categories of Concern

Unfortunately, there are numerous public examples of the significant failures of the current U.S. legal and regulatory system in preventing the loss of critical technology to China. In part, these losses are due to ownership changes in critical American companies through both inbound Chinese investment and outbound U.S. investment to China, which potentially cause harm to U.S. national security.

Beijing's efforts to acquire advanced semiconductor technology such as microprocessors, or the brains of modern electronics, is a sobering example of these failures. Faced with CFIUS' likely blocking of any attempt to buy outright a U.S. microprocessor firm, Beijing has exploited loopholes in both CFIUS and the export control regime to successfully acquire some of these critical technologies. China's goals in acquiring American microprocessor technology are two-fold: (1) subvert current U.S. export controls that prohibit the sale of such advanced chips to be installed in Chinese supercomputers[25] by acquiring the underlying technology and know-how necessary to reproduce the chips indigenously in China, and (2) over the long-term, reduce reliance on American suppliers by fostering a viable and globally competitive domestic industry. Examples of advanced U.S. semiconductor technologies acquired by China in ways that appear to avoid both CFIUS and export controls include:

- *IBM Power8 High-Performance Microprocessor Architecture Technology:* IBM's decided to license elements of the 22nm Power8 high performance server and supercomputer chip architecture to Chinese partners with extensive commercial

---

accessed at:
http://www.uscc.gov/sites/default/files/Peter%20Mattis_Written%20Testimony060916.pdf

[23] William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, London: Routledge, May 2013.

[24] *USCC 2016 Annual Report*, accessed at:
https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf

[25] https://www.theregister.co.uk/2015/04/10/us_intel_china_ban/

relationships with the PRC government.[26] This is the later generation of a chip architecture that previously received hundreds of millions in development funds from DARPA,[27] and is currently deployed in systems to maintain our nuclear arsenal.[28]

- *AMD High-Performance X86 Microprocessor Technology:* AMD licensed its high performance x86 microprocessor design architecture and transfered the necessary know-how needed to replicate this chip to a consortia of shadowy Chinese companies performing supercomputing work for the Chinese military and defense-industrial base.[29] Through the AMD deal, the Chinese government acquired both a back-door to Intel's technology, since much of AMD's and Intel IP is co-shared, and also created potential vulnerabilities in U.S. weapons systems, many of which use x86-based computing systems.[30] Ironically, while AMD assists the Chinese Government in the development of its supercomputers, it is also receiving millions in U.S. taxpayer dollars to develop similar technologies for the U.S. Department of Energy's next generation supercomputer.[31]
- *Qualcomm Advanced 10nm Server Chip Processor Technology:* Qualcomm's Chinese government subsidized joint venture Huaxintong Semiconductor[32] is working to develop high-end server chips based on the worlds most advanced 10nm process node technology.[33]

Other examples outside of the semiconductor space include Microsoft's joint venture with China's defense electronics conglomerate China Electronic Technology Group Corporation,[34]

---

[26] Paul Mozur, "IBM Venture with China Stirs Concerns," *New York Times*, 19 April 2015, accessed at: https://www.nytimes.com/2015/04/20/business/ibm-project-in-china-raises-us-concerns.html.

[27] https://www-03.ibm.com/press/us/en/pressrelease/20671.wss

[28] The beta of Department of Energy's "Sierra" supercomputer is based on the Power 8 chip, and used for nuclear weapons arsenal stewardship. https://computation.llnl.gov/computers/sierra. The final version will be based on the Power9 chip.

[29] Don Clark, "AMD to License Chip Technology to China Chip Venture," *Wall Street Journal*, 21 April 2016, accessed at: https://www.wsj.com/articles/amd-to-license-chip-technology-to-china-chip-venture-1461269701; Jane Perlez, Paul Mozer and Jonathan Ansfield, "China's Technology Ambitions Could Upset the Global Trade Order," *New York* Times, 7 November 2017, accessed at: https://www.nytimes.com/2017/11/07/business/made-in-china-technology-trade.html.

[30]

[31] http://www.amd.com/en-us/press-releases/Pages/amd-selected-by-2017jun15.aspx

[32] David Barboza, "How This Tech Giant is Backing China's Tech Ambitions," *New York* Times, 4 August 2017, accessed at: https://www.nytimes.com/2017/08/04/technology/qualcomm-china-trump-tech-trade.html?mtrref=undefined&gwh=3307243E0E2CB283EF310DDBEBEB2C50&gwt=pay

[33] https://www.qualcomm.com/news/onq/2017/11/08/qa-anand-chandrasekher-discusses-qualcomm-centriq-2400

[34] Gregg Keizer, "Microsoft Partners with Chinese State-Owned Defense Conglomerate to Promote, Sell Windows 10 to Government," *ComputerWorld*, 18 December 2015, accessed at:

which has five numbered institutes on the Department of Commerce's denied entity list for export control violations;[35] and Chinese investment in artificial intelligence company Neurala.[36] Again, in nearly all of these examples, CFIUS did not appear to have jurisdiction over the transaction, nor did export controls effectively limit the loss of critical know-how and IP flowing to Chinese state entities.

Why FIRRMA is Needed

Passage of the proposed Foreign Investment Risk Review Modernization Act (FIRRMA), S.2098, would constitute a significant step in the right direction to reform CFIUS to deal with these new and evolving approaches inherent in China's strategy. FIRRMA offers essential new tools to ensure future transactions:

- Monitors transactions, transfers, agreements, or arrangements designed to evade or circumvent CFIUS and U.S. export controls
- Expands the scope of review to include real estate transactions near sensitive U.S facilities
- Widens the scope of review to include joint ventures and minority-position investments that are "non-controlling" but "non-passive," with the goal of preventing investment-driven transfers of technology or technology "contributions" by the U.S. partner, and also monitors changes in foreign investors' rights, especially increases in ownership percentage after approvals.
- Broadens CFIUS' definition of "critical technologies" to include emerging technologies such as artificial intelligence, robotics, and machine learning that could strengthen another country's military technologies
- Mandates review of transactions in which the foreign entity is more than 25% owned by a foreign government, which is particularly important with Chinese state-owned enterprises[37]

---

https://www.computerworld.com/article/3016921/microsoft-windows/microsoft-partners-with-chinese-state-owned-defense-conglomerate-to-promote-sell-windows-10-to-gove.html

[35] https://www.bis.doc.gov/index.php/forms-documents/regulations-docs/federal-register-notices/federal-register-2014/957-744-supp-4-1/file.

[36] Jonathan Ray, Katie Atha, Edward Francis, Caleb Dependahl, James Mulvenon, Daniel Alderman, and Leigh Ann Ragland-Luce, *China's Industrial and Military Robotics Development*, Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, October 2016, accessed at: https://www.uscc.gov/sites/default/files/Research/DGI_China%27s%20Industrial%20and%20Military%20Robotics%20Development.pdf

[37] While Chinese state-owned enterprises are perennial source of concern, one must not fall into the trap of thinking that private Chinese companies do not participate in state-sponsored technology theft and espionage. Recently, Derek Scissors from the American Enterprise Institute gave the following testimony to the House Financial Services Subcommittee:

"More important, there is no difference in the control the Communist Party can exercise over private firms and SOEs. There is no rule of law in the PRC, no court or media through which

- Changes evaluation criteria to include "whether the transaction involves a country of special concern that has a demonstrated or declared the strategic goal of acquiring a type of critical technology that a U.S. business that is a party to the transaction possesses"
- Adds badly needed new evaluation factors, including cybersecurity threats and protection of personally identifiable information (PII), etc.

These changes would modernize the CFIUS system to keep pace with the changes in China's strategy and its coordinated national technology policies described above, as well as make the process nimble and flexible enough to adapt to future changes in methods.

Notwithstanding assertions that FIRRMA would duplicate export controls, the reality is wildly different. In fact, FIRRMA includes a critical deferral to U.S. export controls, which all agree constitute the first line of defense to protect U.S. national security concerns. This deferral would prevent duplicative reviews and unnecessary burdens on U.S. companies. Thus, to the extent current U.S. export controls are improved in the future, those improvements would reduce the number of transactions subject to CFIUS jurisdiction under FIRRMA. Moreover, CFIUS and the Bureau of Industry and Security, which administers U.S. export controls, have long engaged regularly in the context of CFIUS reviews. The reality is that CFIUS and U.S. export controls are complimentary and do not and should not operate in exclusive domains going forward.

Why U.S. Export Controls Are Not Enough

A common criticism of FIRRMA is that it seeks to expand CFIUS to cover activities already adequately addressed by the current export control system. Yet the export control system has a number of key flaws:

- First, export controls are product and even feature specific and therefore inherently narrow. With enough financial motivation, some U.S. companies may "design-out" or "de-architect" specific aspects of the technology being transferred that would otherwise trigger export controls. This approach is akin to providing China with 70 percent of the latest technology, with China then being able to use its massive financial resources, overseas investment acquisition campaign, and state-sponsored commercial espionage apparatus to quickly close the remaining 30 percent gap. The upshot is that such ventures greatly accelerate the pace of China's ability to master critical technologies that are of vital concern to U.S. national security.
- Second, once a joint venture is launched in China with a controlled technology, engineers of the U.S. company may then come under intense pressure to assist the Chinese partner to address limitations of the controlled technology. This is akin to your auto dealer

---

private Chinese firms can resist Party orders to ignore US law or steal technology. Private Chinese companies receive less in the way of subsidies but are as beholden to the Party for their survival as SOEs are. There is no justification to treat them differently with regard to national security."

https://financialservices.house.gov/uploadedfiles/hhrg-115-ba19-wstate-dscissors-20180109.pdf

putting a speed limiter on a sports car, only for it to be removed easily in the owner's home garage under duress. In short, it is highly unrealistic—even foolhardy—to expect export controls, including deemed exports, to be able to effectively protect against certain transfers of "know-how" from individual engineers or subject matter experts operating inside of a joint venture on Chinese soil. This is particularly the case as one considers the pressures on engineers employed by U.S. companies operating in China given the objectives and actions of the CCP and under increasingly intense CCP control under Xi Jinping.

- Third, the system is not nimble or quick enough to include rapidly emerging, dual-use technologies that could have significant military implications
- Fourth, because the current structure focuses on technology controls rather than transactions, it does not protect adequately against leakage through supply chains or intra-company transfers after ownership or equity changes or combinations into joint ventures.

Moreover, the export control system has been proven to be largely ineffective at identifying proper "risk of diversion" to military entities once the technology has been transferred to China. For example, despite the glaringly obvious risks, export licenses were granted to UTC to sell its military-grade attack helicopter control software to Chinese defense companies.[38] For its part, Intel was initially permitted but later blocked from selling chips to the developers of Chinese military supercomputers.[39] While the U.S. Government took enforcement actions to rectify both of these situations, in both cases it was too late - the technology had already been transferred to China and was key to enhancing Chinese capabilities. The Commerce Department list of denied export entities is also not updated to reflect CFIUS actions – for example, San'an optoelectronics,[40] a Chinese chip firm twice blocked by CFIUS in an attempt to acquire military technology, is still not on the denied entities list, and American firms continue selling sensitive technology to Sanan' directly.[41]

Conclusion

The Chinese government's economic development and technology modernization strategies and policies have created a sub-optimal business environment for U.S. companies in China and presented new challenges to the investment approval, counter-espionage, and export control efforts of the U.S. Government. Passage of FIRRMA in its current form would be a critical step forward in evolving those efforts to protect U.S. national security while still promoting and supporting foreign investment in the U.S. and the ability of U.S. companies to innovate and grow in the China market and globally.

---

[38] https://www.justice.gov/opa/pr/united-technologies-subsidiary-pleads-guilty-criminal-charges-helping-china-develop-new

[39] https://www.theregister.co.uk/2015/04/10/us_intel_china_ban/

[40] https://www.ledinside.com/news/2016/8/gcs_holdings_sell_to_sanan_opto_blocked_by_us_authorities_to_form_joint_venture and https://www.wsj.com/articles/u-s-regulators-move-to-stop-chinese-takeover-of-german-tech-firm-aixtron-1479549362

[41] https://about.keysight.com/en/newsroom/pr/2016/22apr-nrb16060.shtml?cc=FR&lc=fre

While I share the concerns of some that a significant expansion in the scope of CFIUS review must be matched by a commensurate increase in resources, especially additional qualified personnel. the U.S. Congress has always ensured that our national security comes first and ensured adequate funding to ensure technology supremacy on the battlefield and safeguard the homeland. Make no mistake, China's industrial policies, including China's outbound investment campaign and inbound investment coercive tactics designed to acquire technologies that are critical to U.S. national security, represent an exigent threat in both areas, and China is closing any remaining gaps rapidly. It is essential that the Congress work closely with the Administration to ensure that CFIUS is adequately resourced to address this clear and present threat, while ensuring that our CFIUS system operates efficiently and allows the foreign direct investment that is important to driving growth and creating jobs at home.