March 19, 2021

STATEMENT OF HON. NAZAK NIKAKHTAR

Partner, International Trade and National Security Practice, Wiley Rein LLP;

Former Assistant Secretary for Industry & Analysis and Under Secretary for Industry & Security, U.S. Department of Commerce

Testimony Before the United States-China Economic and Security Review Commission*

U.S. Investment in China's Capital Markets and Military-Industrial Complex

Chairman Bartholomew and Vice-Chairman Dr. Cleveland, hearing Co-Chairs Commissioner Borochoff and Commissioner Fiedler, and all Commissioners, thank you for the opportunity to speak about the extent to which the People's Republic of China's (PRC or China) access to U.S. and global capital poses risks to U.S. economic, foreign policy, and national security interests.

My name is Nazak Nikakhtar, and it is an honor to appear before you today. I am an international trade and national security attorney at the Washington, DC, law firm of Wiley Rein LLP. I am also a trade and industry economist, a former Georgetown University adjunct law professor, and I recently completed my second tour of duty in the U.S. Government. Twenty years ago, I began my career as an analyst at the U.S. Department of Commerce's Bureau of Industry and Security and subsequently at the International Trade Administration, where my colleagues and I witnessed from the frontlines the predatory economic tactics used by our trading partners to hollow-out our industries. In 2004, I helped institute Commerce's China/Non-Market Economy Office and, for several years thereafter, I audited numerous foreign (including Chinese) companies and their affiliates for the Department. In 2018, I returned to the Commerce Department to serve as Assistant Secretary for Industry & Analysis and, in 2019, I simultaneously served, performing the non-exclusive functions and duties, as the Under Secretary for the Bureau of Industry and Security. It is from all of these vantage points that I offer my testimony and observations today.

U.S. policymakers and leaders around the world have increasingly described the PRC's military buildup as a threat to the national security, economic security, and foreign policy interests of the United States and its allies. Today, the PRC is the world's second largest economy, and

**The views and opinions expressed in this testimony are mine only and do not represent the views of Wiley Rein LLP or any of the firm's clients.*

some analysts project that the Chinese economy will surpass that of the United States by 2028.[1] The key reason we are discussing the PRC's military industrial complex today is because the strength of the PRC's military is directly linked to the country's economic growth, and this has alarming implications for the Chinese Communist Party's (CCP) geopolitical power and ability to carry out its global intentions. Hong Kong provides us with a small glimpse into what may happen. It is time to take these challenges seriously and take decisive and proactive measures to protect our national security.

I. THE CCP, PEOPLE'S LIBERATION ARMY (PLA), AND THE CHINESE COMMUNIST MILITARY COMPANIES (CCMC): QUEST FOR GLOBAL SUPREMACY

A. The Growth of the PLA

The PLA is the military arm of the PRC's ruling Communist Party. It is well documented that, since 1978, the CCP has been engaging in a sustained and aggressive effort to transform the PLA from a low-technology and infantry-heavy apparatus to a high-technology force that is able to rival any other military in the world. In 1999, Congress recognized the growing threat that the PLA posed and, in response, through the National Defense Authorization Act (NDAA), directed the Department of Defense (DOD) to begin identifying CCMCs and simultaneously authorized the President to exercise authorities under the International Emergency Economic Powers Act (IEEPA) to counter any resulting national security threat.[2]

Yet, for 20 years thereafter, notwithstanding the steady accumulation of power and resources, superior technological progress, and operational sophistication of the Chinese military,

---

[1] BBC, *Chinese Economy to Overtake US by 2028 due to Covid* (Dec. 26, 2020), https://www.bbc.com/news/world-asia-china-55454146.

[2] Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, Pub. L. No. 105-261, § 1237, 112 Stat. 1920 (1998) ("1999 NDAA"), https://www.govinfo.gov/content/pkg/PLAW-105publ261/pdf/PLAW-105publ261.pdf. The NDAA authorizes the Secretary of Defense to determine CCMCs in consultation with the Attorney General, the Director of Central Intelligence, and the Director of the Federal Bureau of Investigations. The CCMC provision of the 1999 NDAA was updated in 2021 by the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (2021), § 1260(H), https://www.congress.gov/bill/116th-congress/house-bill/6395/text ("2021 NDAA"). The 2021 NDAA includes requirements for annual reports on the U.S. operations of companies linked to the PLA (§ 1260H) and a report on China's military capabilities and activities in the Arctic (§ 8424).

the U.S. Government did not produce the CCMC list.[3] It was not until June 2020 that the DOD issued its "initial" list of CCMCs and committed to "continue to update the list with additional entities as appropriate."[4] The initial tranche identified 20 CCMCs operating directly or indirectly in the United States. Between June 2020 and January 2021, the list more than doubled to 44 companies.[5] More work needs to be done.

The 2021 NDAA amends the 1999 NDAA and defines CCMCs as entities "owned, controlled, or beneficially owned by, or . . . acting as an agent of or on behalf of" the PLA or an organization subordinate to the CCP's Central Military Commission, *or* entities that are identified as "military-civil fusion contributor[s] to the Chinese industrial base," who are also "engaged in providing commercial services, manufacturing, producing, or exporting."[6] "Military-civil fusion contributor[s]" are those entities that contribute in very specific ways to the "Chinese defense industrial base."[7] As set forth below, this definition should be amended in order to facilitate the designations of additional PRC companies that aid the PLA and the PRC's military industrial complex.

The PLA is two million strong, and the U.S. Government has now recognized that the growth and magnitude of the PRC's economic and military capabilities are "the primary concern in U.S. national security."[8] The DOD's 2018 National Defense Strategy observes that a central part of the CCP's global strategic ambitions is to weaken the economies of its competitors.[9] More recently, in its 2020 report to Congress on Military and Security Developments Involving the

---

[3] Press Release, Department of Defense Newsroom, DOD Releases List of Additional Companies, In Accordance with Section 1237 of FY99 NDAA (Jan. 14, 2021).

[4] *Id.*

[5] On March 12, 2021, the DC District Court preliminary enjoined the DOD's designation of Xiaomi Corporation as a CCMC due to insufficient evidence under the Administrative Procedure Act.

[6] 2021 NDAA Sec. 1260(H)(d).

[7] *Id.*

[8] Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States*, U.S. Department of Defense (2018) at 1, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[9] *Id*. at 1-3.

People's Republic of China, the DOD underscores that the PRC is rapidly moving to complete its goal of realizing military and economic hegemony.[10]

It is well established that the PLA's strength has been fueled by the CCP's coercive and market-distortive behaviors that drive the country's own technological and economic advancements and, by design, destroy the competitive positions of non-Chinese actors. As the DOD acknowledges, such tactics include, in addition to rampant intellectual property (IP) theft, "commercial joint venture requirements, technology transfer requirements, subsidies to lower the cost of inputs, sustaining excess capacity in multiple industries, sector-specific limits on foreign direct investment, discriminatory cybersecurity and data transfer rules, insufficient intellectual property rights enforcement, inadequate transparency, and lack of market access."[11] These predatory practices, compounded by the enormous amount of funds that steadily pour into the PRC economy through foreign capital, tilts the playing field *in favor* of China and *against* the United States and its allies. Indeed, the culmination of these factors compelled the DOD to conclude last year that "China has already achieved parity with – or even exceeded – the United States in several military modernization areas."[12] The DOD and the Congressional Research Service summarized a number of these areas as follows:[13]

- **PLA Navy:** "An approximately 350-ship navy that includes advanced platforms such as submarines, aircraft carriers, and large multi-mission surface vessels, giving China blue-water capabilities and the ability to conduct sustained operations and project power increasingly far from China's periphery."[14] "In comparison, the U.S. Navy's battle force is approximately 293 ships as of early 2020. China is the top ship-producing nation in the world by tonnage and is increasing its shipbuilding capacity and capability for all naval classes."[15]

---

[10] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2020* ("DOD 2020 Report to Congress"), https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

[11] *Id.* at 12-13.

[12] *Id*. at vii.

[13] Caitlin Campbell, *China Primer: The People's Liberation Army (PLA)* (Jan 5, 2021), Congressional Research Service ("CRS PLA Report") at 1-2.

[14] *Id.* at 1.

[15] DOD 2020 Report to Congress at vii.

- **PLA Air Force:** The PRC's air force together with the navy's aviation "constitute the largest aviation forces in the [Indo-Pacific] region and the third largest in the world, with over 25,000 total aircraft and approximately 2,000 combat aircraft. The [PLA Air Force] is rapidly catching up to Western air forces across a broad range of capabilities and competencies."[16] The PLA's air force is "increasingly capable of conducting joint and over-water missions, featuring deployments of large numbers of fourth-generation fighters, and fifth-generation fighters becoming operational or in late stages of development."[17]

- **PLA Rocket Force:** "The PRC has one of the world's largest forces of advanced long-range surface-to-air systems – including Russian-built S-400s, S-300s, and domestically produced systems – that constitute part of its robust and redundant integrated air defense system (IADS) architecture."[18] "A conventional missile force designed to enable China to deter or defeat possible third-party intervention in a regional military conflict, and featuring around 100 intercontinental ballistic missiles and hundreds of theater-range conventional missiles, including anti-ship ballistic missiles designed to target adversary aircraft carriers; and a nuclear force intended to be small but survivable (DOD estimates China's nuclear stockpile is in the 'low-200s' and likely to at least double in the coming decade), with progress toward a 'nuclear triad' (including land-, submarine-, and aircraft-launched nuclear weapons)."[19] "The PRC has developed its conventional missile forces unrestrained by any international agreements. The PRC has more than 1,250 ground-launched ballistic missiles (GLBMs) and ground-launched cruise missiles (GLCMs) with ranges between 500 and 5,500 kilometers. The United States currently fields one type of conventional GLBM with a range of 70 to 300 kilometers and no GLCMs."[20]

- **PLA Strategic Support Force:** "A force that centralizes cyber and space capabilities (referred to by the PRC as the 'new commanding heights in strategic competition') as well as electronic and psychological warfare."[21]

- **PLA Joint Logistics Support Force:** "A force that facilitates joint logistics across the PLA to enable large-scale military operations."[22]

---

16 *Id.* at viii.

17 CRS PLA Report at 1.

18 DOD 2020 Report to Congress at vii.

19 CRS PLA Report at 2.

20 DOD 2020 Report to Congress at vii.

21 CRS PLA Report at 2.

22 *Id.*

The DOD warns, moreover, that the PLA's capabilities are expected to increase as the PRC ramps up its "intensive campaign to obtain foreign technology" through "illicit means" and other strategies including "imports, foreign direct investment, talent recruitment, and R&D and academic collaborations."[23] The CCP's ultimate objective is to "roll back American power" and become the preeminent economic and military superpower globally.[24] As summarized by Kevin Rudd, the former prime minister of Australia, the PRC is well-positioned to achieve this goal:

> [I]n both reality and in perception, China has already become a more important economic partner than the United States to practically every country in wider East Asia. We all know where the wider strategic logic takes us. From economic power proceeds political power, from political power proceeds foreign-policy power, and from foreign-policy power proceeds strategic power. That is China's strategy.[25]

B. CCP's Aggressive Growth Strategy

It has been widely reported that the CCP mandates and coerces – through law, administrative guidelines, and regulations – commercial and non-commercial entities to transfer sensitive information, trade secrets, and intelligence information to the central government. In addition, PRC laws require that entities conform their practices to advance the CCP's military and economic interests.[26] In fact, the CCP's Military-Civil Fusion strategy demands that entities cooperate with the government to advance the military strength and power ambitions of the PLA. All PRC entities, even those enterprises that still remain ostensibly private and civilian, are legally obligated to serve the state and the CCP such that PRC entities have limited autonomy over their business decisions. The PRC's routine installation of CCP officials inside private firms ensures compliance with the central government's mandates.[27] The reality today is that PRC entities

---

[23] DOD 2020 Report to Congress at 149.

[24] Ben Sasse, *The Responsibility to Counter China's Ambition Falls to US*, The Atlantic (Jan. 26, 2020), https://www.theatlantic.com/ideas/archive/2020/01/china-sasse/605074/.

[25] Kevin Rudd, *Understanding China's Rise under Xi Jinping*, Sinocism (Mar. 17, 2018), https://sinocism.com/p/understanding-chinas-rise-under-xi-jinping-by-the-honourable-kevin-rudd.

[26] U.S. China Business Council, *Fact Sheet: Communist Party Groups in Foreign Companies in China*, China Business Review (May 31, 2018), https://www.chinabusinessreview.com/fact-sheet-communist-party-groups-in-foreign-companies-in-china/.

[27] Lingling Wei, *China's Xi Ramps Up Control Over Private Sector*, Wall Street Journal (Dec. 10, 2020), https://www.wsj.com/articles/china-xi-clampdown-private-sector-communist-party-11607612531.

operate in a military-driven ecosystem that is centrally coordinated by the CCP to advance the state's economic growth, weapons capabilities, intelligence operations, and security apparatuses.

Moreover, the CCP's One Belt, One Road initiative encourages the expansion of the PLA's geopolitical reach globally. Under this initiative, the CCP is acquiring stakes in strategic industries and supporting infrastructure in many countries, such as key transportation ports in Greece, railways in Ethiopia, mines in Africa, and massive steel plants in Indonesia and India. These investments augment the CCP's military presence and economic control abroad and, as noted in the United States' 2017 National Security Strategy, these investments can serve as "persuasion" for nations to follow the CCP's directions.[28] The extent of such overseas investments also evidences the CCP's *modern colonization* of strategic regions.

The CCP views data as another strategic domain of military and economic competition that must be controlled and leveraged to advance the country's power ambitions. The Department of Homeland Security observes that the CCP's coercive and illicit acquisition of sensitive data from foreign sources, including intellectual property of foreign governments/private enterprises and personally identifiable information of individuals worldwide, is a central driving force in the PRC's bid to solidify its position as a leading global military and technological superpower by 2049.[29] The objective of the CCP's data accumulation strategy is to hasten the demise of foreign competitors and to fast-track the PRC's technological dominance in key strategic sectors such as aerospace, artificial intelligence (AI) systems, cyber intelligence, biometrics, genomics, semiconductors, pharmaceutical medicines, and energy.[30] In furtherance of these goals, the CCP has instituted a number of laws mandating that Chinese and foreign companies transfer sensitive IP, proprietary commercial secrets, and personal data to the central government and the PLA, including:

---

[28] President Donald J. Trump, *National Security Strategy of the United States*, The White House (2017) at 46, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[29] U.S. Department of Homeland Security, *Data Security Business Advisory: Risk and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China* (Dec. 22, 2020) ("DHS Advisory") at 3, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[30] *Id.* at 4.

- **National Security/Intelligence Laws:** mandates the transfer of data, information, and technology to PRC authorities.[31]

- **Cybersecurity Law:** mandates that network operators cooperate with public security organs. [32]

- **Cryptography Law:** any system with a CCP "approved" encryption must provide its encryption keys to the government. [33]

- **Data Security Law (implementation pending):** empowers CCP authorities to demand data from companies and requires companies to "favor economic and social development in line with the CCP's social morality and ethics." [34]

- **Export Control Law:** prohibits exports of "important data," essentially any information (including R&D developed by foreign-owned companies) outside of China.[35]

These laws appear to apply to all companies operating in China, regardless of nationality and, in some instances, they also appear to have extraterritorial application, reaching to corporate operations abroad.

Finally, in order to compel businesses to adhere to these and other similar legal mandates, the CCP instituted last year a nationwide social credit rating system for all corporations to detect misconduct and non-compliance. [36] The "Corporate Social Credit System" has implications for companies operating in China – whether foreign-owned or domestic – with respect to proprietary technical information, sensitive personal data, and surveillance information. Companies may be given low scores if they fail to transfer their internal data to the CCP as part of their obligations. Failing to score well, by non-compliance with the government's policies or demands, may subject companies to a myriad of sanctions, including higher taxes or permit difficulties, or a blacklisting

---

31 *Id.* 6-7.

32 Lauren Maranto, *Who Benefits from China's Cybersecurity Laws?*, Center for Strategic & International Studies (June 25, 2020), https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.

33 DHS Advisory at 8-9.

34 *Id.* at 7-8.

35 *Id.* at 8; Ck Tan, *China's Export Control Law to Become 'Key Dynamic' in U.S. Relations*, Nikkei Asia (Dec. 1, 2020), https://asia.nikkei.com/Economy/China-s-export-control-law-to-become-key-dynamic-in-US-relations.

36 *See, e.g.*, Michael D. Sutherland, *China's Corporate Social Credit System*, Congressional Research Service (Jan. 17, 2020), https://crsreports.congress.gov/product/pdf/IF/IF11342; Kendra Schaefer, *China's Corporate Social Credit System: Context, Competition, Technology and Geopolitics*, Trivium China (Nov. 16, 2020), https://www.uscc.gov/sites/default/files/2020-12/Chinas_Corporate_Social_Credit_System.pdf.

which could mean financial ruin.[37] The European Chamber of Commerce describes this credit rating system as potentially amounting to "life or death" for companies operating in China.[38]

Today, the legal and policy levers that the CCP utilizes to force entities to contribute to the advancement of the PRC's military industrial complex continue to expand. Indeed, the PRC government is now better-suited than ever to efficiently harness the power of data and technology, as well as the country's own massive economy, population, manufacturing base, and R&D capabilities, to accelerate its military in size and performance capabilities in order to overpower any non-Chinese nation.

II. U.S. CAPITAL FLOWS INTO THE PRC AND PLA

The CCP's laws and policies are not the only drivers of growth for the PLA and the PRC's military industrial complex. The transfer of capital from the United States, and indeed from the rest of the world, are also contributing heavily to the technological and operational buildup of the PLA. According to the U.S.-China Economic and Security Review Commission, in October 2020, there were 217 Chinese companies listed on NASDAQ, the New York Stock Exchange (NYSE) and NYSE American, with a combined market capitalization of $2.2 trillion.[39] In 2020, Chinese-based companies raised approximately $11.7 billion in the United States through 30 initial public offerings. This represents the highest amount of capital raised since 2014, when Alibaba went public as the biggest IPO.[40]

Further, publicly available data indicate that the United States imported approximately $451 billion in goods and services from the PRC in 2020.[41] The aggregate value of these imports

---

[37] *Id.* at sec. 4.

[38] European Chamber of Commerce, *European Chamber Report on China's Corporate Social Credit System, A Wake-Up Call for European Businesses in China* (Aug. 28, 2019), https://www.europeanchamber.com.cn/en/press-releases/3045/european_chamber_report_on_china_s_corporate_social_credit_system_a_wake_up_call_for_european_business_in_china.

[39] U.S.-China Economic and Security Review Commission, *Chinese Companies Listed on Major U.S. Exchanges* (Oct. 2, 2020), https://www.uscc.gov/research/chinese-companies-listed-major-us-stock-exchanges#:~:text=As%20of%20October%202%2C%202020,the%20three%20major%20U.S.%20exchanges.

[40] Cheng, Evelyn, *China-based Companies Raised $11.7 Billion Through U.S. IPOs This Year, the Most Since 2014*, CNBC (Dec. 18, 2021), https://www.cnbc.com/2020/12/18/china-based-companies-raise-the-most-money-via-us-ipos-since-2014.html (citing data from Renaissance Capital).

[41] U.S. Department of Commerce, International Trade Administration.

represents capital flows into China. Additionally, U.S. public and private equity investments in Chinese and Hong Kong domiciled companies totaled over $2.3 trillion dollars in market value of holdings at the end of 2020. Investments in Chinese and Hong Kong companies listed on Commerce's Entity List (a list of foreign entities subject to significant U.S. trade restrictions due to national and foreign policy concerns) totaled nearly $49 billion by market value.[42] Investments in state-owned enterprises (SOEs) in China and Hong Kong totaled over $152 billion by market value. Investments in CCMCs totaled nearly $48 billion and investments in Military End User (MEU) companies (another list of foreign entities subject to significant U.S. trade restrictions) stood at nearly $6.5 billion. Investments in the banned mobile apps, which were the subject of the January 5, 2021 Executive Order (EO), including Alipay and Tencent,[43] totaled nearly $650 billion.

By sector, nearly $43 billion of U.S. capital has been invested in Chinese and Hong Kong telecommunications companies, over $1.3 billion in robotics companies, $50 billion in biotechnology companies, nearly $1.3 billion in aerospace and defense companies, $21 billion in semiconductor companies, $31 billion in pharmaceutical companies, $221 billion in AI companies, and $45 billion in data companies.

We need to consider these data points against the fact that, according to the Hurun Global Unicorn List issued in August 2020, of the 586 unicorns globally – startups valued at over $1 billion – China had 227 unicorns (up from 206 unicorns in 2019) compared with 233 for the United States (up from 203 in 2019).[44] Many of these unicorns in China represent technologies in key emerging sectors that threaten to undermine the United States both in terms of economic competitiveness and national security. AI, for example, is one of the largest sectors in the listing. Chinese doctrine has stressed AI as a lynchpin of future economic and military power, and of course it is the technology driving China's social and corporate credit systems. China has 21

[42] U.S. Department of Commerce Entity List, at Supplement No. 4 to Part 744, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

[43] Exec. Order No. 13971, 86 Fed. Reg. 1,249 (Jan. 5, 2021), https://www.federalregister.gov/documents/2021/01/08/2021-00305/addressing-the-threat-posed-by-applications-and-other-software-developed-or-controlled-by-chinese.

[44] *Hurun Global Unicorn Index 2020*, Hurun Research Institute (Aug. 4, 2020), https://www.hurun.net/en-US/Info/Detail?num=E0D67D6B2DB5.

unicorns in this critical sector and the United States has 35. In fintech, China has 18 while the United States has 21, but the cumulative valuation of these Chinese unicorns is $239 billion while the United States stands at only $84 billion. Further, of the top 10 unicorns in 2020, the largest four are Chinese firms: Ant Group, ByteDance, Didi Chuxing, and Lufax. By contrast, the largest U.S. unicorn is SpaceX holding the number five position. The United States represents only four unicorns on the top ten list (with a cumulative valuation of $133 billion), whereas Chinese firms account for the remaining six (with a cumulative valuation of $378 billion). It is also worth underscoring again that all of these Chinese unicorns – like all Chinese companies – are subject to a patchwork of national security-oriented laws that allow Chinese security and intelligence services to effectively leverage Chinese firms for sensitive data, espionage, and other purposes.[45]

Further, American state and pension fund holdings in Chinese and Hong Kong companies totaled nearly $15 billion at the end of 2020, of which nearly $1.1 billion were invested in SOEs. Of course, when U.S. individual and institutional investors invest in Chinese firms, they may not be aware that they are funding companies involved in activities that are contrary to U.S. interests, including companies that appear on the Commerce Department's Entity List and CCMCs.

Finally, it is worth noting that the $2.3 trillion of U.S. investments in Chinese and Hong Kong companies should be considered in conjunction with China's disclosed defense budget, which stood at $178.6 billion in 2020 (this is second only to the United States),[46] as should U.S. equity investments in CCMCs, which represented 27 percent of this $178.6 billion figure. Furthermore, although many speculate that this $178.6 billion figure is significantly understated, the figure still does not capture the value of capital that flows from the CCP as subsidies to the PRC's commercial sector or the massive volume of foreign equity that pours into the PRC's business enterprises. Given that all commercial companies are mandated by the CCP to advance the growth of the PRC state and its military, it should come as no surprise that much of the U.S. capital transfers to the PRC are, in significant ways, aiding the PLA's technological and operational advancements as well. So too is capital from foreign sources worldwide. Put

[45] For instance, per Article Seven of China's 2017 National Intelligence Law, private Chinese companies are compelled to cooperate in "state intelligence work." Furthermore, these laws require data to be housed inside China, as well as require random inspections and black-box security audits.

[46] CRS PLA Report at 2.

differently, the more the United States and its allies transfer capital to the CCP, the more we fund the growth of the PLA and the PRC's larger military industrial complex and, consequently, the more we undermine the growth and strength of our own industries and national defense. This is astounding. In this zero-sum game, we should be funding innovation and technological advancements in the United States and the nations of our allies.

III. CURRENT U.S. POLICIES AND POTENTIAL FOR FURTHER ACTION

Juxtaposing the enormous size of capital flows into Chinese firms against the backdrop of the DOD's warnings about the growth of the CCP and the PLA, the gap in the United States' approach to national security policy becomes quite obvious. Fundamentally, as a nation, we need to ask whether we perceive the CCP's economic and military might as posing a risk to U.S. and global national security interests. If the answer is "yes," then we must determine the extent to which we are willing to enact policies that curtail our contributions to the CCP's growth.

Given that the CCP itself views its Military-Civil Fusion strategy as melding the commercial and military sectors into the same intertwined state-coordinated apparatus, then logic dictates that we ought to take the same view. This means coming to terms with the reality that our business dealings with the Chinese commercial sector have aided the growth of CCP's military industrial complex for the last forty years. Even business dealings where we service PRC industries' demand in low-technology commodity sectors are not benign, but rather create opportunities for the Chinese economy to shift resources away from low-technology enterprises to higher-technology sectors to accelerate indigenization and, in many instances, ramp up production scale. Many of us have witnessed firsthand these dynamics taking place and the ensuing hollowing-out of industries around the world. These are the realities underpinning our bilateral trading relationship; maintaining the status quo cannot be our strategy going forward.

If the United States Government, lawmakers, and citizens ultimately heed the DOD's warnings and conclude that the CCP's military industrial complex does indeed pose a threat to our national security and the security of our allies, then we need to quickly identify all legal authorities that may be used to decelerate our contributions to the CCP's and PLA's growth from both the standpoints of capital flows and transfer of critical technologies.

A. Legal Implications of CCMC Designations Under NDAA

It is important to note that, while the CCMC lists that the DOD produces pursuant to the NDAA are not sanctions lists themselves, the identification of CCMCs, as noted above, did cause the President to impose restrictions on such entities, pursuant to Section 1237 of the 1999 NDAA on November 12, 2020, by issuing EO 13959. This EO prohibits U.S. persons from engaging in transactions in publicly-traded securities of CCMCs (or securities that are derivative of, or designed to provide investment exposure to such securities). The EO cited national security, foreign policy, and economic concerns over U.S. investments in these companies in light of China's Military-Civil Fusion strategy, [47] and invoked IEEPA authority to address such concerns.[48] That EO remains in effect today.[49]

The CCMC designation has other legal implications as well, namely for U.S. government contractors and other companies participating in the U.S. Government's supply chain. For example, the Federal Acquisition Regulations (FAR) prohibit U.S. Government agencies from "procuring or obtaining" "any equipment, system, or service" that utilizes "covered telecommunications equipment or services" for certain critical technology or a "substantial or essential component of any system."[50] Although the FAR identifies several Chinese companies as being subject to the prohibitions, the regulations nevertheless apply to any other company "that the Secretary of Defense . . . reasonably believes to be an entity owned or controlled by, or

---

[47] Exec. Order 13959, 85 Fed. Reg. 73,185 (Nov. 12, 2020), https://www.federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies, *as amended by* Exec. Order 13974 (Jan. 13, 2021), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-amending-executive-order-13959-addressing-threat-securities-investments-finance-communist-chinese-military-companies/. EO 13959 observes that the PRC, through the Military-Civil Fusion strategy, "increases the size of the country's military industrial complex by compelling civilian Chinese companies to support its military and intelligence activities" and "aid their development and modernization." Additionally, the EO notes that the PRC pressures U.S. index providers and funds "to include these securities in market offerings, and engaging in other acts to ensure access to United States capital," and thereby exploits U.S. investors in order to "finance the development and modernization" of the Chinese military.

[48] The EO also authorizes the Department of Defense, in consultation with the Department of Treasury, to designate CCMCs as well as the Department of Treasury's Office of Foreign Assets Control.

[49] EO 13959 was amended on January 13, 2021 by EO 13974 (clarifying dates for divestment and other technical corrections), https://www.federalregister.gov/documents/2021/01/19/2021-01228/amending-executive-order-13959addressing-the-threat-from-securities-investments-that-finance.

[50] Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services of Equipment, 85 Fed. Reg. 42,665 (July 14, 2020), https://www.govinfo.gov/content/pkg/FR-2020-07-14/pdf/2020-15293.pdf.

otherwise connected to, the government of a foreign country.[51] Moreover, the DOD's supplement to the FAR (the Defense Federal Acquisition Regulation Supplement) prohibits the acquisition of items covered by the United States Munitions List from a CCMC.[52]

Further, Section 514 of the Consolidated Appropriations Act for 2018 specifies that for "high-impact or moderate-impact" information systems, agencies must review the "supply chain risk," including the risk related to cyber-espionage or sabotage by entities identified by the U.S. Government "including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China."[53]

The CCMC list designation was also recently referenced in the Department of Commerce's December 23, 2020 final rule on export licenses to MEUs. Therein, the Department of Commerce's Bureau of Industry and Security (the unit charged with export controls on dual-use items) identified specific MEUs and announced that they would be subject to enhanced export licensing requirements under the Export Administration Regulations. Although only the Aviation Industry Corporation of China (AVIC) is listed both as a MEU and a CCMC, the agency nevertheless cautioned that other CCMCs (as well as other non-listed parties) could be military end users (or require licenses for items that are restricted for "military end uses") and that additional due diligence ought to be exercised by potential exporters to determine whether export restrictions apply.[54]

Finally, in any transaction that may be regulated by the U.S. Government, including procurement, federal agencies are authorized to exercise broad discretion in undertaking assessments of national security risks if CCMCs are involved. That said, in light of the small

---

[51] FAR, Section 4.2101(4).

[52] Defense Federal Acquisition Regulation Supplement, Pub. L. No. 112-181, at sec. 225.770.

[53] Consolidated Appropriations Act, Pub. L. No. 115-141, 132 Stat. 348, 439 (2018), https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

[54] *Military End User List*, U.S. Department of Commerce, Bureau of Industry and Security, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/1770.

number of CCMCs identified by the DOD to date (44 entities),[55] the Government's ability to fully address national security risks under these authorities is limited.

B. Improving the NDAA's Framework for CCP Designations

The 2021 NDAA expanded the definition of CCMCs and thereby presumably sought to enhance the DOD's ability, through CCMC designations, to keep pace with the CCP's and PLA's increasing control over the Chinese commercial sector and the CCP's rapid rise as the United States' number one national security threat.[56] Congress should consider additional amendments to the NDAA to further improve the DOD's CCMC designation authority.

First, the NDAA should not limit the definition of CCMCs to only those entities that provide "commercial services, manufacturing, producing, or exporting."[57] The reality is that CCMCs are also engaged in a range of other activities including engineering, R&D, technology development and deployment, data accumulation, computer coding, cloud computing, and non-commercial financial and logistics services that strengthen the PLA's operations and capabilities. The NDAA's scope should be expanded to capture all such activities as well.

Second, the NDAA's framework for CCMC designations appears to require "substantial evidence" under the Administrative Procedure Act to meet its definitional requirement, *i.e.,* that entities are "directly or indirectly" acting "on behalf of the PLA" or the "Central Military Commission," or that CCMC entities are "military-civil fusion contributor[s]" to the Chinese defense industrial base.[58] To the extent that the compilation of substantial evidence is required, then this would prolong and potentially frustrate, rather than facilitate, the designation of many CCMCs. Moreover, the current definition of CCMCs – *i.e.,* that "military-civil fusion contributor[s]" be entities linked in very specific ways to certain Chinese military institutions *rather than all military and CCP institutions* – is too narrow. It does not reflect the myriad of

---

[55] As noted, the designation of Xiaomi Corporation as a CCMC has been preliminarily enjoined pending final court order, *supra* n. 5.

[56] News Release, *China Poses Largest Long-Term Threat to U.S., DOD Policy Chief Says*, U.S. Department of Defense (Sept. 23, 2019), https://www.defense.gov/Explore/News/Article/Article/1968704/china-poses-largest-long-term-threat-to-us-dod-policy-chief-says/.

[57] 2021 NDAA, Sec. 1260H(d)(1)(B)(ii).

[58] *Id.*, Sec. 1260H(d)(1)(B)(i).

ways that entities may contribute to the operations and technological advancements of the PRC's military industrial complex beyond the criteria laid out in the NDAA. Hence, the narrow definition may prevent CCMC designations that are warranted.

The law should *facilitate* rather than impede the identification of CCMCs that pose national security threats. Here, Congress should consider amending the NDAA by instituting a "reasonable cause to believe" standard similar to the standard for including a foreign company on the Department of Commerce's Entity List.[59] This more flexible standard would facilitate the designation of CCMCs by reducing the evidentiary burden on the DOD and would reduce litigation risk for the Government as well.

Finally, and in light of the extensive levels of CCP-mandated integration and coordination across the PRC's commercial and military sectors, it may be reasonable to consider applying a *de jure* approach (rather than a *de facto* approach) for designating CCMCs. The reality is that the PRC's "Military-Civil Fusion" policy and national security laws require that all commercial and military entities operating in China help advance the objectives of the CCP, PLA, and other factions of the Chinese government. These laws, on their face, warrant the *de jure* designation of most PRC companies operating in strategic sectors as CCMCs without the need for any additional factfinding. Given that a *de jure* legal framework is able to more readily and expeditiously produce CCMC designations, capture more CCMC entities due to its broader legal reach, and facilitate the DOD's process for such designations, the NDAA should be amended.

C. Additional Recommendations for Action

To supplement the foregoing recommendations for future NDAA amendments, Congress and the Administration should consider exploring additional legal authorities to counter the wide range of threats posed by the CCP, PLA, and the PRC's expanding military industrial complex. At the outset, available data indicate that the volume of capital flowing from the United States to the PRC, and ultimately to the CCP and PLA, through financial investments and trade is extensive,

[59] 15 C.F.R.§ 744.11(b) ("Entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entity has been involved, is involved, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States and those acting on behalf of such entities may be added to the Entity List . . . .").

but it is not accurately tracked. The United States should institute a system that better tracks capital flows in a manner that is accurate, timely, and transparent, and we should encourage our allies to do the same. Indeed, whenever capital from Americans and allied nations are transferred to dangerous actors in *any* country, we must have a better understanding of the nature, scope, and scale of the problem in order to appropriately address it. We are not quite there yet.

Second, Congress's new Holding Foreign Companies Accountable Act, which was signed into law on December 18, 2020, represents a significant step forward in curbing America's exposure to financial risks when dealing with foreign companies listed on U.S. exchanges. This Act not only requires that listed companies declare that they are not owned or controlled by a foreign government, but the law also mandates that companies disclose to the United States Securities and Exchange Commission information on foreign jurisdictions that prevent the Public Company Accounting Oversight Board (PCAOB) from conducting inspections. The PCAOB has publicly acknowledged that it has been "prevented" by the CCP "from inspecting the U.S.-related audit work and practices of PCAOB-registered firms in . . . China, and, to the extent their audit clients have operations in mainland China, Hong Kong."[60] This has resulted in investors often not having a reliable picture of Chinese companies' financial health, and ultimately having to bear the resulting fallout associated with the lack of disclosure and difficulty in pursuing legal recourse. Under the Act, such companies will be banned from trading and delisted from U.S. exchanges if the PCAOB is unable to perform specific audits for three consecutive years. The PCAOB should be vigilant in its audits since accounting fraud runs rampant in the PRC.

Third, the Government's use of IEEPA authority in November 2020 to counter the threats posed by CCMCs, including restrictions on U.S. investments in CCMCs as described in the November 2020 EO 13959, as amended by the January 2021 EO 13974, is another step in the right direction. To broaden the scope of this ban, earlier this month, Senators Rubio and Kennedy introduced legislation entitled the American Financial Markets Integrity and Security Act to prohibit "malign Chinese companies" – including the parent, subsidiary, affiliate or the controlling entity – that are listed on the Department of Commerce's Entity List or the DOD's CCMC list,

[60] Public Company Accounting Oversight Board, Oversight/International, Updated List of Issuer Audit Clients of Firms in Jurisdictions Where the PCAOB Has Been Denied Access to Conduct Inspections, https://pcaobus.org/oversight/international/international/inspections/062011_updatedinformation.

from accessing U.S. capital markets.[61] Congress's forward-leaning approach to solving these complex issues should be commended, and additional legislation should be encouraged to protect U.S. citizens and investors from exploitation by all malign actors.

The fourth item addresses U.S. transfers of technology to high-threat actors. Although the Export Control Reform Act of 2018 (ECRA) legislated the protection of "emerging technologies" through the use of export controls, the debate continues in the U.S. Government as to the most effective way to implement ECRA's mandates and restrict such exports. At the outset, there is widespread recognition that emerging technologies are most vulnerable to foreign acquisition when they are at the nascent stages of development. Congress recognized this reality when it used the term "emerging" in ECRA. Indeed, at the nascent stage of development, the full range of applications that may arise from new technology are seldom identified. Because Congress recognized this uncertainty, it instituted regulatory controls over their exports given that the same technologies that wield the power to drive significant advancements in the commercial sector may also be exploited for both known and yet-to-be known dangerous uses by foreign adversaries. AI is a perfect example of this intersection.

My understanding is that the U.S. Government appreciates the enormous difficulty associated with the task of identifying "emerging technologies" for export controls when those technologies and their applications are constantly evolving. The Government further recognizes that, in order to move forward with controls, it must decide between two very different types of regulatory approaches. The first option is to wait until "emerging" technologies develop into somewhat better understood, more "mature" technologies in order to be more precisely defined for controls (in much the same way that most technologies are identified on export control lists). Alternatively, the U.S. Government has the option of acting more swiftly by delineating and controlling broader categories of technologies as "emerging technologies" under ECRA.

---

[61] Senator Rubio's Press Release, *Rubio, Colleagues Introduce Legislation Banning Harmful Chinese Companies from Exploiting U.S. Capital Markets*, (Mar. 3, 2021), https://www.rubio.senate.gov/ public/index.cfm/press-releases?id=B9291EF7-5B5C-4DE9-8A56-1972D12E9014; Senator Kennedy's Press Release, *Kennedy, Rubio introduce bill banning dangerous Chinese companies from exploiting U.S. capital markets* (Mar. 3, 2021), https://www.kennedy.senate.gov/public/2021/3/kennedy-rubio-introduce-bill-banning-dangerous-chinese-companies-from-exploiting-u-s-capital-markets.

I do not believe that the U.S. Government has abandoned either option to date, even though there are downsides associated with each. The former approach, whereby "emerging technologies" are narrowly defined, risks additional delay in instituting controls that are presently needed. Moreover, by attempting to define technologies that are not yet fully understood with a high degree of specificity, the Government may inadvertently omit necessary technologies from control. A too-narrow definition also increases the likelihood of circumvention by technology developers who may be able to reconfigure their technologies in minor ways in order 'design out' from the scope of controls. On the other hand, the alternative approach of adopting a broader definition of "emerging technologies" – while it allows for the more expeditious implementation of licensing requirements – runs the risk of regulating more exports than necessary to protect national security. To the extent the U.S. Government adopts either option, it should consider imposing licensing requirements for only exports of emerging technologies to entities and/or countries that pose the most significant national security risks. When the acquisition of emerging technologies by U.S. allies does not pose risks, allies could be exempt from licensing requirements. This approach eases the licensing burden on federal agencies and U.S. businesses.

Fifth, although the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) also represented a major milestone in protecting national security by providing the Committee on Foreign Investment in the United States (CFIUS) with enhanced authority to protect "critical technologies" from foreign acquisition through foreign direct investments (FDI), the U.S. Government has not yet been able to fully utilize this new authority. This is because FIRRMA's definition of "critical technologies" rests in large part on ECRA's identification of "emerging technologies," and until the U.S. Government makes progress on this issue, gaps in our national security laws persist.

Here too, the question of whether to narrowly or broadly define "emerging technologies" has important implications in the context of reviews of FDI transactions. On one hand, a broader definition would subject a wider range of transactions to FIRRMA authority, thereby giving the U.S. Government increased visibility into U.S. FDI activities and greater authority to restrict those that threaten national security. On the other hand, it is argued that increased regulatory oversight will deter FDI flows into the United States. To address this latter concern, the U.S. Government could consider limiting mandatory filing requirements to only those entities and/or countries that

pose the most significant threats to U.S. national security. This would decrease regulatory burdens on U.S. businesses and ultimately reduce the volume of transactions subject to review by federal agencies.

Whichever option the U.S. Government pursues has serious implications. But the ultimate point here is that the U.S. Government needs to make substantial progress in its identification of "emerging technologies" under ECRA and "critical technologies" under FIRRMA. Movement on these fronts will give businesses some clarity going forward and enable the U.S. Government to fully exercise the legal authorities it possesses to protect national security. The exercise of those authorities has, for two years, languished.

Sixth, in much the same way that FIRRMA and its predecessor, the Foreign Investment and National Security Act of 2007, imposed national security reviews on inbound FDI transactions, Congress seems to be considering similar legislation for outbound investments to high-risk countries. New legislation would call for CFIUS-type reviews of U.S. capital flows to foreign markets – whether through public exchanges or private equity – for national security risks. Again, to lessen the burden on U.S. businesses in filing notices of such transactions for federal agency review and to ease the workload for U.S. Government agencies adjudicating such transactions, the scope of reviews could be limited to outbound transactions involving only foreign entities and/or countries that pose the most significant national security risks.

Seventh, the U.S. Government should develop a comprehensive, consistent, and complementary legal standard for evaluating the extent to which commercial and non-commercial foreign entities are controlled by or affiliated with their provincial or central governments. The lack of a comprehensive framework has, to date, significantly impeded the U.S. Government's analysis in export controls, FIRRMA investment screenings, intelligence community risk assessments, federal government acquisitions, and supply chain vulnerability analyses. This shortcoming ought to be remedied, and the solution is quite simple. Congress should, by legislation, adopt the longstanding legal definitions of affiliation that exist in U.S. international trade laws, through statute, regulations, and case precedent, and apply these definitions to augment the legal authorities currently existing across all federal agencies. The trade laws extend the definition of affiliation beyond ownership interests to the broad range of ways in which foreign

governments are able to exercise influence over corporate entities' business operations such that the entities lose autonomy over key decisions. These trade laws have been upheld by U.S. courts for decades, are consistent with the United States' obligations under the World Trade Organization agreements, and will therefore withstand judicial scrutiny. Of course, the application of a comprehensive legal standard such as this would improve each federal agency's ability to maximize the use of its own existing authorities where a determination of affiliation is needed. Further, a consistent legal approach such as this would promote uniformity and predictability across the U.S. Government agencies' legal authorities, and provide better clarity to businesses seeking regulatory approvals.

Finally, there is often little convergence across the various lists of sanctioned entities issued by the U.S. Government, including the Treasury Department's Specially Designated Nationals and Blocked Persons Lists, the Commerce Department's Entity List and MEU list, and the DOD's CCMCs lists. In some instances, this separation makes sense given that various sanctions are governed by different legal authorities and standards. In other instances, where the legal standards overlap, it makes sense to harmonize the lists. Further, many regulatory reviews of transactions involving these entities could be assessed under a presumption or policy of denial, to the extent the U.S. Government considers that these entities pose serious national security risks. Greater transparency in the regulatory process would provide certainty to U.S. businesses and improve consistency in the U.S. Government's approach to protecting national security.

IV. CONCLUSION

I would like to conclude with a note of caution. It is widely known that the PRC controls the supply of materials that are most essential to our defense capabilities, including critical minerals, metals and rare earths, and lithium-ion battery cells. The reason the CCP has not restricted our access to these materials yet, although it has threatened to do so, is because the PRC continues to be dependent on our highly-advanced semiconductor technology. Once, however, the PRC achieves semiconductor parity with the United States – a certainty, which is as little as four to five years away – the CCP will be perfectly positioned to withhold these materials in order to

force the United States and other countries to bend to its will. Should this happen, our defense capabilities will be crippled.

We ought to keep in mind that the CCP has made amply clear – through the tremendous size and pace of the PLA's military modernization efforts – that it is preparing for some significant form of power confrontation with the United States and the rest of the world. Time is not on our side, and we must take every step necessary to preserve our national security interests.

I look forward to your questions.