

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051
<https://oversight.house.gov>

May 6, 2024

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Ave. NW
Washington, D.C. 20535

Dear Director Wray:

The Committee on Oversight and Accountability (Committee) is investigating the Chinese Communist Party's (CCP or the Party) political warfare operations and the Federal Bureau of Investigation's (the Bureau or FBI) response to this ongoing threat. As a result of the delay or "inexcusable failure to recognize the threat" from the People's Republic of China (PRC), "the greatest national security challenge is now before the U.S."¹ This warrants urgent attention from the FBI.

Cybersecurity and new technologies are the "defining national and economic security challenges of the 21st century," and therefore are "increasing both the kinds of sensitive information that can be stolen and the complexity of the threat landscape."² You have previously acknowledged that CCP cyber-warfare efforts target our critical infrastructure and position the Party to "wreak havoc and cause real world harm to American citizens and communities" at a time of their choosing, leaving our national and economic security vulnerable.³ The Committee is seeking more information on how the Bureau is protecting the nation from CCP warfare, particularly the CCP's illicit attempts to control the technology and artificial intelligence that is central to our country's security and infrastructure and necessary for a prosperous future.

¹ James E. Fanell & Bradley A. Thayer, *Embracing Communist China, America's Greatest Strategic Failure* (2024) at 124 ("It is difficult to comprehend the enormity of the blunder, but Americans must, while facing the cold truth that it happened.").

² U.S. House of Representatives, *China Task Force Report*, (Sep. 2020) at 56.

³ *The CCP Cyber Threat to the American Homeland and National Security: Hearing Before H. Sel. Comm. on the Chinese Communist Party*, 118th Cong. ("CCP Cyber Threat Hearing") (Jan. 31, 2024) (Statement of Christopher Wray, Dir., Fed. Bureau of Invest.).

Broader Committee Investigation

The Committee is conducting oversight of the federal government's work to protect the American people from CCP political warfare⁴ and nefarious influence operations. For decades, the CCP has sought to infiltrate and influence every aspect of American society.⁵ The CCP's goal is plain: defeat the "main enemy," which counterintelligence officials have identified as America.⁶ The fronts are multiple; according to the CCP itself: "[t]he battlefield will be everywhere."⁷ And the tools are myriad, with the "united front"⁸ leading as one of the PRC's⁹ "magic weapons,"¹⁰ as described by General Secretary Xi Jinping,¹¹ to advance the Party's aim of global domination.¹² United front work (UFW), which may be executed by the United Front Work Department (UFW) or elsewhere in the Party, is a "unique blend of engagement, influence activities, and intelligence operations" that the CCP uses to "influence other countries' policy toward the PRC and to gain access to advanced foreign technology."¹³ UFW "generally involves covert activity and is a form of interference that aids the CCP's rise."¹⁴ United front "networks" are used "to carry out relationship-focused influence campaigns through a multitude of proxies."¹⁵

Despite years of false promises to the West, the CCP openly seeks to achieve its destructive ambition. In 1999, two People's Liberation Army Air Force colonels authored *Unrestricted Warfare*, which has been described as a strategic military vision for the PRC to

⁴ "Political warfare seeks to influence emotions, motives, objective reasoning, and behavior of foreign governments, organizations, groups, and individuals in a manner favorable to one's own political-military objectives." Mark Stokes, *The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics*, Project 2049 Inst. (Oct. 14, 2013).

⁵ See generally Constantine C. Menges, *China The Gathering Threat* (2005); H.R. Rep. No. 105-851 (1999) ("Cox Report"); Robert Spalding, *War Without Rules* (2022); Col. Grant Newsham, *When China Attacks: A Warning to America* (2023); Kerry K. Gershaneck, *Political Warfare: Strategies for Combating China's Plan to "Win without Fighting"* (2020); see also Larry Diamond & Orville Schell, *China's Influence & America's Interests: Promoting Constructive Vigilance*, Hoover Inst. (2019).

⁶ Menges, *supra* note 5; Gershaneck, *supra* note 5 ("The PRC is engaged in war against the United States. It is not mere competition or malign influence, but war by PRC definition."); Newsham, *supra* note 5, at 60 (The CCP "seeks global domination" and "will fight its main enemy, the United States, to achieve it.").

⁷ Qiao Liang & Wang Xiangsu, *Unrestricted Warfare: China's Master Plan to Destroy America* (PLA Lit. & Arts Pub. House 1999) (China) (military colonels describing twenty-four varieties of warfare).

⁸ "While the CCP's United Front Work Department has functional responsibility for these [warfare] operations and activities, PRC united front work is a task of all CCP agencies and members." Gershaneck, *supra* note 5, at 22.

⁹ It is essential to understand that Xi Jinping has removed any "veneer of separation between the [CCP] and the Chinese state." Gershaneck, *supra* note 5, at 43 (quoting Ann-Marie Brady, *Exploit Every Rift: United Front Work Goes Global*, in David Gitter et al., *Party Watch Annual Report*, Ctr. for Adv. China Res. (2018)).

¹⁰ Ann-Marie Brady, *Magic Weapons: China's political influence activities under Xi Jinping*, Wilson Ctr. (Sept. 18, 2017); see also Sel. Comm. on the Chinese Communist Party, *Memorandum: United Front 101*, at 7 ("United Front 101 Memo").

¹¹ Alex Joske, *The party speaks for you: Foreign interference and the Chinese Communist Party's united front system*, Austl. Strategic Pol'y Inst. (Jun. 09, 2020) (quoting Xi Jinping at 2015 Central United Front Work Meeting).

¹² See, e.g., Newsham, *supra* note 5, at 43 ("The People's Republic of China may settle for dominance rather than occupation, but it does indeed aim to rule us all.").

¹³ United Front 101 Memo, *supra* note 10, at 1.

¹⁴ Joske, *The party speaks for you*, *supra* note 11, at 19.

¹⁵ Alex Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World*, at 63 (2022).

defeat America through political warfare.¹⁶ Retired Brig. Gen. Robert Spalding, who has served in senior positions in strategy and diplomacy with the U.S. Departments of Defense and State for decades, characterizes the book as “the main blueprint for China’s efforts to unseat America as the world’s economy, political, and ideological leader,” which “shows exactly how a totalitarian nation set out to dominate the West through a comprehensive, long-term strategy that includes everything from corporate sabotage to cyberwarfare to dishonest diplomacy; from violations of international trade law and intellectual property law to calculated abuses of the global financial system.”¹⁷ Kerry Gershaneck, former counterintelligence officer who wrote a seminal book on combatting PRC Political Warfare, has explained that *Unrestricted Warfare* details CCP use of “any methods” where “the boundaries between war and non-war and between military and non-military affairs [have] systemically broken down.”¹⁸ To successfully combat these highly organized and pervasive warfares spawned by China, federal agencies must first recognize and understand them.

The CCP “know[s] the strength of the American people, of the American idea, and that’s why China has launched so many warfares to try to weaken us, divide us, and get us to hate ourselves and each other.”¹⁹ Retired Col. Grant Newsham, former U.S. Marine Liaison Officer to the Japan Ground Self-Defense Force and U.S. Foreign Service Officer, has advised that “the way out of this is to rediscover why we are an exceptional country, get to know each other better, and fight side by side.”²⁰

As all Americans are targets of the PRC’s warfare,²¹ federal agencies have responsibilities to (1) conduct outreach to citizens about the dangers they may encounter, and (2) provide appropriate incentives for Americans to proactively protect themselves—their communities, schools, houses of worship, businesses, finances, food, and more—from the threat. Federal agencies must prepare Americans to “take action.”²² To stop the CCP’s “destructive actions,” retired Brig. Gen. Spalding advises that it will “take macrolevel strategic changes by our government, but also microlevel actions by individuals, businesses and other civic

¹⁶ Gershaneck, *supra* note 5.

¹⁷ Spalding, *War Without Rules*, *supra* note 5, at xii; *see also* Robert Spalding, *Stealth War*, at 12-13 (2019) (*Unrestricted Warfare* “should be required reading for all branches of the US government and for business leaders, because it outlines, in no uncertain terms, the strategy behind China’s policies,” including stating that the “new principles of war” are “no longer ‘using armed force to compel the enemy to submit to one’s will,’ but rather are ‘using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one’s interests.’”).

¹⁸ Gershaneck, *supra* note 5, at 16 (quoting Qiao Liang & Wang Xiangsu, *supra* note 7, at 6-7).

¹⁹ Newsham, *supra* note 5, at 341.

²⁰ *Id.*

²¹ “The Three Warfares, the traditional foundation of PRC political warfare, include public opinion/media warfare, psychological warfare, and legal warfare.” Gershaneck, *supra* note 5. It “requires efforts to unify military and civilian thinking, divide the enemy into factions, weaken the enemy’s combat power, and organize legal offensives.” Elsa Kania, *China Brief: The PLA’s Latest Strategic Thinking on the Three Warfares*, Jamestown Found. (Aug. 22, 2016).

²² Spalding, *War Without Rules*, *supra* note 5, at 214.

institutions.”²³ The Committee is surveying each agency’s role to secure Americans and their communities.

Congress has recognized the threat posed by the PRC for some time. Notably, in 1999, the U.S. House Select Committee on U.S. National Security and Military/Commercial Concerns with the People’s Republic of China concluded that in the preceding decade, the PRC used a “variety of techniques including espionage, controlled commercial entities, and a network of individuals that engage in contact with scientists, business people and academics” as part of its warfare operations.²⁴

With varying degrees of effort and success, federal agencies have sought to address the CCP’s attack on what Col. Newsham has aptly described as “[t]he core of America.”²⁵ However, the threat is grave and work must be done across agencies to protect America.²⁶ Peter Mattis, former staff director of the Congressional-Executive Commission of China and counterintelligence analyst at the CIA counsels that

Only by being clear in public about the actions and intentions of the Chinese party-state, and being publicly accountable for the actions the U.S. government takes in response, will the United States be able to address Beijing’s challenges while upholding our democratic commitment to fair, transparent justice for all Americans.²⁷

To this end, the Committee is conducting this investigation and implores each federal agency to uphold its duty to the American communities for whom they are responsible.

Securing America’s Technological Infrastructure

The FBI’s stated mission to protect and defend the United States against foreign intelligence threats and cyber-based attacks is of paramount importance in a time where all aspects of society revolve around technology.²⁸ As Gen. Spalding has explained, data and technology “provide the most chillingly efficient authoritarian weapons for controlling populations.”²⁹ The CCP is actively leveraging this reality via attacks on American cyber operations, data, artificial intelligence (AI), and the economy. These attacks represent a whole-

²³ *Id.*; see also Peter Mattis & Matt Schrader, *America Can’t Beat Beijing’s Tech Theft With Racial Profiling*, War on the Rocks (July 23, 2019) (“The U.S. government’s difficulties in telling a convincing story about the Chinese Communist Party point to a[n] important step: addressing a serious lack of ‘China literacy,’ both within the enforcement portions of the federal bureaucracy, and in U.S. society as a whole.”).

²⁴ Cox Report, *supra* note 5, at xxxiii; see generally Menges, *supra* note 5.

²⁵ Newsham, *supra* note 5, at 33.

²⁶ See Newsham, *supra* note 5, at 309 (“We need to know, value, protect and build the strengths of the United States of America, and shed the light of truth on the corruption, in every sense of the word,” of the CCP. “That could mean in discussions with family, community, at school or wherever that understanding needs bolstering.” Education courses on PRC political warfare would benefit “[a]ny decision-makers who work with China.”); see Gershaneck, *supra* note 5, at 153 (outlining such courses to “build[] internal defenses”).

²⁷ Mattis & Schrader, *supra* note 23.

²⁸ See FBI, *Mission and Priorities*, available at <https://www.fbi.gov/about/mission>; MPS: Functions Manual: FBI, available at <https://www.justice.gov/archive/jmd/mps/2009omf/manual/fbi.htm>.

²⁹ Spalding, *Stealth War*, *supra* note 17, at 179.

of-society threat, with the potential to severely disrupt critical infrastructure, personal and government data, the economy, and America’s ability to lead the Fourth Industrial Revolution, which represents a fundamental change in the way we live, fueled by digital transformation in manufacturing and production (further described below).³⁰

CCP warfare of this kind could be catastrophic for Americans. As explained by the U.S.-China Economic and Security Review Commission, the CCP’s cyber operations “pose a serious threat to U.S. government, business, and critical infrastructure networks in the new and highly competitive cyber domain.”³¹ Amidst America’s technological reliance on the functioning of daily infrastructure, CCP warfare against critical infrastructure “represent[s] real world threats to our physical safety.”³² Infrastructure is the “underlying foundation that society needs to function,” and Gen. Spalding has explained that the CCP uses infrastructure projects as “unassuming, innocuous, but powerful weapons to gain influence over potential allies and rivals alike.”³³ Infrastructure warfare may, in fact, be “the most subtle and most corrosive of [the CCP’s] unrestricted aggressions.”³⁴ Gen. Spalding warns that a “wholesale breakdown or even partial collapse of any one of [these foundations] would lead to catastrophic events almost immediately.”³⁵

Malicious CCP cyber-attacks target virtually every sector of America, including “healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms.”³⁶ If the CCP gains access to networks controlling these critical sectors, “*it would be able to weaponize the technology within entire cities—or entire countries—served by that network and hold that city or state at its mercy.*”³⁷ The FBI has important responsibilities to warn and protect Americans from critical infrastructure hacks, which have been characterized as the “cyber space equivalent of placing bombs on American bridges, water treatment facilities, and power plants.”³⁸

³⁰ See *What is Industry 4.0?*, IBM, available at <https://www.ibm.com/topics/industry-4-0>.

³¹ U.S.-China Economic and Security Review Commission, Section 2: China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States, at 418.

³² CCP Cyber Threat Hearing, *supra* note 3 (Statement of Christopher Wray, Dir., Fed. Bureau of Invest.).

³³ Spalding, *Stealth War*, *supra* note 17, at 162.

³⁴ *Id.* at 163.

³⁵ *Id.* at 162.

³⁶ Newsham, *supra* note 5, at 194 (quoting *China Cyber Threat Overview and Advisories*, Cyber and Infrastructure Security Agency (2022)).

³⁷ Spalding, *Stealth War*, *supra* note 17, at 115 (emphasis in original).

³⁸ CCP Cyber Threat Hearing, *supra* note 3 (Statement of Chairman Mike Gallagher); see also FBI Director Christopher Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, FBI News, Hudson Institute, Video Event: China’s Attempt to Influence U.S. Institutions (July 7, 2020).

CCP Cyber Warfare & The Fourth Industrial Revolution

CCP cyber warfare specifically targets Americans' data. Data's immense value has been explained by David Goldman, Deputy Editor for the *Asia Times* and Washington Fellow at the Claremont Institute's Center for the American Way of Life: "If computation is the engine, data is the fuel."³⁹ Goldman, an American economic strategist, has met with Chief Technology Officer, Paul Scanlan, of Huawei, a PRC telecommunications giant and the world industry leader in telecommunications equipment.⁴⁰ Scanlan openly acknowledged to Goldman that Huawei's technological global ambitions are "longer range," with research centers in twenty-one different countries.⁴¹ Goldman explains that Huawei might be one of the CCP's most important weapons for its global ambitions, and observed that it has blatantly advertised the CCP's plan for "global economic supremacy" since 2011.⁴² Huawei was recognized as a threat to America as early as 2012 and was identified as a global national threat by national security advisor Robert O'Brien in 2020.⁴³

The PRC's willingness to steal and illegally harvest sensitive data, through Huawei's global reach and other means, threatens America's ability to take control of what experts have referred to as the "Fourth Industrial Revolution." The Fourth Industrial Revolution fundamentally changes manufacturing and production, and is based largely on "[a]rtificial intelligence applied to big data sets."⁴⁴ It is characterized by "increasing automation and the employment of smart machines and smart factories,"⁴⁵ and has been described as a "fusion of technologies that is blurring the lines between the physical, digital, and biological spheres."⁴⁶ The CCP's goal to lead the Fourth Industrial Revolution encompasses a takeover of "not only the sinews of the new industrial age, but scores of spinoff applications that will transform manufacturing, mining, healthcare, finance, transportation, and retailing—virtually the entirety of economic life."⁴⁷ If the CCP does lead the Fourth Industrial Revolution, Goldman warns that the "consequences for the United States will be disastrous: we will become considerably poorer, our politics will be less stable, and our economy will be dominated by an adversary."⁴⁸

³⁹ David P. Goldman, *How America Can Lose the Fourth Industrial Revolution*, Claremont Institute Center for the American Way of Life (Nov. 11, 2021) at 5-6 ("While the control point of the twentieth-century economy was oil, the control point of the twenty-first is data.").

⁴⁰ See Linda Hardesty, *Huawei turns the corner on profits in 2023*, Fierce Wireless (Mar. 29, 2024).

⁴¹ David P. Goldman, *You Will be Assimilated* 39-40 (2020).

⁴² David P. Goldman, *The Chinese Challenge: America has never faced such an adversary*, Claremont Review of Books (Spring 2020) ("Huawei provides the template for the new Chinese empire.").

⁴³ See Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (Oct. 8, 2012); Fox Business, *Huawei poses global national security threat: Robert O'Brien* (Feb. 21, 2020) (5:12 – 6:00); Julian Barnes, *White House Official Says Huawei Has Secret Back Door to Extract Data*, *The New York Times* (Feb. 11, 2020).

⁴⁴ Goldman, *How America Can Lose the Fourth Industrial Revolution*, *supra* note 39, at 5.

⁴⁵ IBM, *supra* note 30.

⁴⁶ Goldman, *How America Can Lose the Fourth Industrial Revolution*, *supra* note 39, at 5.

⁴⁷ Goldman, *The Chinese Challenge*, *supra* note 42.

⁴⁸ Goldman, *How America Can Lose the Fourth Industrial Revolution*, *supra* note 39, at 1.

As we have seen, the CCP relentlessly deploys hacking missions to access American databases and steal information. The Party's record of *successfully* stealing American data is alarming. In 2014, CCP hackers illegally retrieved more than 21 million records from the federal government's Office of Personnel Management.⁴⁹ Most recently, the Cybersecurity and Infrastructure Security Agency discovered a PRC state-sponsored cyber group called "Volt Typhoon," allowing CCP hackers to pre-position themselves inside U.S. government systems for years, and granting the CCP the ability to plant disruptive and destructive cyber activity within the nation's critical infrastructure.⁵⁰ The FBI and other federal agencies must protect America from the CCP's efforts to "loot[] U.S. government and private industry networks of strategic data [] and sector-dominating trade secrets," before damage becomes irrevocable.⁵¹

CCP Technological Theft and Espionage in the Age of Artificial Intelligence

The National Security Commission on Artificial Intelligence has concluded that AI will transform every aspect of our existence.⁵² The CCP's AI ambitions, nefarious technological endeavors, and persistent cyber warfare efforts threaten American security, technology, and agency in a digital world. With access to copious amounts of data, often gathered illicitly as discussed above, the CCP has the ability to use AI to "tailor phishing attempts to gain access [to American networks] and steal intellectual property."⁵³ Goldman distills the CCP's intentions as a "campaign for world technological leadership [that] is so ambitious that we still don't get it."⁵⁴

The CCP's willingness and ability to steal data via cyber warfare is particularly troubling for American workers and businesses, especially small businesses, which account for over 45 percent of U.S. employees.⁵⁵ Small businesses are crucial to every sector of the economy, but they are also "the exact firms least likely to invest in state-of-the-art cyber security."⁵⁶ Thus, they are an attractive target for CCP cyber hacks and information theft. The Bureau has

⁴⁹ See Majority Staff Report, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, H. Comm. on Oversight and Gov't Reform (Sep. 2016); Mike Levine, *22 Million Affected by OPM Hack, Officials Say*, ABC News (July 9, 2105).

⁵⁰ Alert, *CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance*, Cybersecurity & Infrastructure Security Agency (Feb. 7, 2024).

⁵¹ Newsham, *supra* note 5, at 193.

⁵² Final Report, National Security Commission on Artificial Intelligence (2021) at 255.

⁵³ Dr. Benjamin Jensen, "How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy", Written Statement before the H. Comm. on the Judiciary, Subcomm. on Courts, Intellectual Property, and the Internet (Oct. 19, 2023) at 2.

⁵⁴ Goldman, *You Will Be Assimilated*, *supra* note 41, at 81-82 ("We're playing power checkers and China is playing Go—an ancient board game of slow and inexorable encirclement, whose objective is to choke off the opponent's ability to move.").

⁵⁵ 2023 Small Business Profile, *United States*, U.S. Small Business Administration Office of Advocacy (Nov. 2023) ("Small businesses are generally defined here as firms with fewer than 500 employees.").

⁵⁶ Jensen, *supra* note 53, at 2.

recognized that the “stakes could not be higher” and the “potential economic harm to American businesses and the economy as a whole almost defies calculation.”⁵⁷

The U.S. must maintain its competitive technological edge, especially since the PRC “has the resources to recruit scientists [and] even steal technology and knowledge.”⁵⁸ The PRC’s reliance on American technological products is steadily declining and CCP espionage efforts are unabating. According to leaked information about a 2022 CCP government directive, there is a push for the CCP to “Delete America,” by muscling American technology out of the PRC and compelling the use of PRC-owned companies.⁵⁹ The CCP wants to sever its technological reliance on America and replace it with its own products, which could mean America will “keep slipping further behind in the [PRC] market.”⁶⁰ Meanwhile, CCP espionage persists, especially relating to AI. A PRC national working at Google was recently arrested for stealing over 500 confidential files containing proprietary AI technology, “while covertly working for [CCP]-based companies seeking an edge in the AI technology race.”⁶¹ National and economic security are in jeopardy due to the “lengths affiliates of companies based in the [PRC] are willing to go to steal American innovation.”⁶²

In its illicit efforts to weaken America and surpass U.S. leadership on the world stage, the CCP focuses on the acquisition of emerging technologies, including quantum computing and 5G networks, which “are poised to enable new growth in AI capabilities.”⁶³ Quantum communications, which can be used to secure data in an “ultra-secure communication network,”⁶⁴ have been described as the “Holy Grail of data security,” because information channels are protected by means of quantum cryptography and interference is easily revealed.⁶⁵ If the CCP uses warfare tactics to gain access to a “fault-tolerant” quantum computing system before the U.S.—meaning a system able to perform calculations with low logical error rates—“we could see mass decryption of sensitive government data and the illicit acquisition of industry trade secrets” beyond what has already been witnessed.⁶⁶ This would give the CCP an unprecedented competitive advantage and enhance its goal to overtake the U.S. as the world’s dominant power by 2049, the year that marks the centennial of the CCP revolution.⁶⁷ Quantum computing, coupled with access to substantial amounts of data, would revolutionize major

⁵⁷ Wray, *supra* note 38 (“It’s the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history.”).

⁵⁸ Ernestas Naprys, *China vs US: who’s winning the race for AI supremacy*, Cyber News (Nov. 28, 2023).

⁵⁹ Liza Lin, *China Intensifies Push to ‘Delete America’ From Its Technology*, Wall St. J. (Mar. 7, 2024).

⁶⁰ *Id.*

⁶¹ Press Release, *Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google*, U.S. Dep’t of Justice Office of Public Affairs (Mar. 6, 2024) (quoting Deputy Attorney General Lisa Monaco).

⁶² *Id.*

⁶³ Final Report, *supra* note 52, at 254-55.

⁶⁴ Martin Giles, *Explainer: What is quantum communication?*, MIT Technology Review (Feb. 14, 2019).

⁶⁵ Goldman, *You Will Be Assimilated*, *supra* note 41, at 110.

⁶⁶ Rob Hays, *From semiconductors to quantum computing: What the US can learn from past oversight*, The Hill (Sep. 23, 2023).

⁶⁷ *Id.*; John Mauldin, *China’s Grand Plan To Take Over The World*, Forbes (Nov. 12, 2019).

industries like logistics, healthcare, finance, and engineering—a potentially devastating outcome if first in the control of the CCP.⁶⁸

The CCP also exploits America’s open research environment and growing economy through “cyber-enabled intrusion, talent recruitment programs, and manipulated research partnerships.”⁶⁹ Under the guise of “fostering legitimate sharing and collaboration,” talent programs usually involve “undisclosed and illegal transfers of information, technology, or intellectual property.”⁷⁰ Since 2008, the CCP’s unrelenting quest for technological supremacy has been extended through a talent recruitment program called the “Thousand Talents Program,”⁷¹ which has since been revived under a different name, “Qiming.”⁷² The program deliberately targets America’s “critical sectors, companies, and research institutions,” by offering salaries, honoraria, research funding, and other monetary support for scientists and foreign nationals to transfer knowledge and information to the CCP.⁷³ These blatant thefts of information and intelligence “feed right into China’s development of artificial intelligence tools” and put American economic security at risk.⁷⁴ Regardless of what these programs are called, they pose a continuing threat to American taxpayer funded research and intellectual property, to which federal agencies must handle with “an effective interagency strategy.”⁷⁵ American technology, data, human agency, and the ability to thrive culturally and economically are all at stake and, importantly, do not belong in the hands of the CCP.

Conclusion and Requests

The FBI bears great responsibility in proactively protecting Americans from CCP threats to national security, which are increasing in both intensity and complexity. Gen. Spalding has explained that “[o]ur leaders have a moral obligation to understand what’s happening, sound the alarm, wake up the country, and inspire Americans of all political stripes to do everything in their power to stop this totalitarian regime.”⁷⁶ The Committee is requesting more information

⁶⁸ Hays, *supra* note 66.

⁶⁹ Final Report, *supra* note 52, at 225.

⁷⁰ Counterintelligence, *The China Threat: Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage*, FBI, available at <https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans>.

⁷¹ Talent Recruitment Office, *Thousand Talents Plan Professorship for Young Scholars*, University of Science and Technology of China, available at <https://employment.ustc.edu.cn/cn/enindexnews.aspx?infoID=665597358281250024>.

⁷² Benzinga, *China’s Stealth Revival Of ‘Thousand Talents Plan’ Signals Semiconductor Ambitions Despite US Restrictions*, Business Insider (Aug. 24, 2023).

⁷³ Final Report, *supra* note 52, at 225; Wray, *supra* note 37 (“...the Chinese government tries to entice scientists to secretly bring our knowledge and innovation back to China—even if that means stealing proprietary information or violating our export controls and conflict-of-interest rules.”).

⁷⁴ Wray, *supra* note 38.

⁷⁵ Staff Report, *Threats to the U.S. Research Enterprise: China’s Talent Recruitment Plans*, Permanent Subcomm. on Investigations, United States Senate (Nov. 18, 2019) at 8.

⁷⁶ Spalding, *War Without Rules*, *supra* note 5, at xvi.

about how the FBI is using an “all-tools and all-sectors approach” in response to the ongoing CCP threat, in order to “protect our nation’s innovation, ideas, and way of life.”⁷⁷

To assist the Committee in investigating this matter, we request a briefing from the FBI with Committee staff. Please contact Committee staff as soon as possible, but no later than May 13, 2024. This briefing should address the following:

- (1) How the FBI strives to inspire and equip Americans to strengthen their communities, innovate, and create the technologies and phenomena that will secure a strong and prosperous future for our nation;
- (2) How FBI leadership ensures from the top down that all FBI employees are aware of CCP warfare and influence operations in America, and are equipped to address them wherever they arise;
- (3) FBI efforts to thwart the CCP threat to American cybersecurity, advancements in artificial intelligence, and quantum computing;
- (4) FBI efforts to brief and warn American communities about the CCP threat and the risks of talent recruitment plans, including but not limited to state and local governments, businesses, universities, and laboratories;
- (5) FBI’s efforts and proposals to inform, prepare, and equip Americans to handle cyber attacks from the CCP, including but not limited to personal and business capacities;
- (6) Vetting procedures of FBI personnel, both at the onset of hiring and periodically, to systematically monitor and address any unlawful ties personnel may have to the CCP;
- (7) FBI efforts to implement or offer widespread training about the CCP’s tactics, methods, and goals to better assist the U.S. government in identifying CCP warfare and articulating an effective interagency response to it; and
- (8) How the Foreign Influence Task Force implements its three-pronged approach to CCP threats, which includes investigation and operations, information and intelligence sharing, and private sector partnerships, without suppressing free speech or violating the First Amendment.⁷⁸

⁷⁷ Wray, *supra* note 38.

⁷⁸ See *Missouri v. Biden*, No. 3:22-CV-01213, 2023 U.S. Dist. LEXIS 114585 (W.D. La. July 4, 2023) (holding that there were plausible claims for government-induced censorship by multiple defendants, including the FBI, the White House, the Surgeon General, the Centers for Disease Control, National Institute of Allergy and Infectious Diseases, and the State Department, which would constitute violations of the First Amendment.) (“...the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable”) (quoting *Matal v. Tam*, 582 U.S. 218, 243 (2018)). This case has been consolidated with *Kennedy v. Biden*, No. 3:23-CV-00381, 2024 U.S. Dist. LEXIS 26751 (W.D. La. Feb. 14, 2024), and is currently pending in the U.S. Supreme Court.

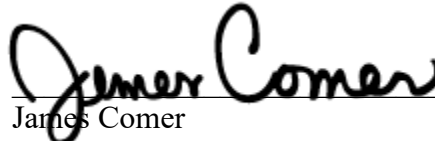
The Honorable Christopher Wray

May 6, 2024

Page 11 of 11

Please contact Committee staff at (202) 225-5074 to schedule the staff briefing. The Committee on Oversight and Accountability is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X. Thank you for your prompt attention to this important investigation.

Sincerely,

A handwritten signature in black ink that reads "James Comer". The signature is written in a cursive style with a large, prominent "J" and "C".

James Comer

Chairman

Committee on Oversight and Accountability

cc: The Honorable Jamie B. Raskin, Ranking Member
Committee on Oversight and Accountability