Written Statement

Before the

House Committee on Small Business

Hearing on

"Defending Main Street: Combating CCP Threats to America's Small Businesses"

Tom Lyons

The 2430 Group

March 25, 2026

I. Introduction

Good morning, Chairman Williams, Ranking Member Velázquez, and distinguished members of the Committee. My name is Tom Lyons. I am a former CIA officer and the co-founder of a small business called the 2430 Group. The 2430 Group is a non-profit, non-partisan organization that educates companies, research institutes, and universities and defends their innovation from nation-state economic espionage attacks. I am here today because America's small businesses are under attack and most of them do not know it.

We have long characterized the Chinese Communist Party as a strategic competitor. But we need to ask ourselves whether their behavior looks like that of a competitor—or that of a nation at war. These are two very different things, and they prompt very different policy responses. The evidence my organization will present today should inform that judgment.

In 1999, two colonels in the People's Liberation Army published a book called *Unrestricted Warfare*, arguing that the future of conflict would be waged through economic subversion, legal manipulation, cyber intrusion, and the systematic theft of a rival's technological advantage. The book itself was never formally adopted as PLA doctrine. But its core concepts were operationalized through formally adopted frameworks, most importantly the PLA's Three Warfares doctrine and its civil-military fusion policy.

In 2003, the Chinese Communist Party's Central Military Commission adopted the "Three Warfares" doctrine—public opinion warfare (公开战), psychological warfare (心理战), and legal warfare (法律战). These are formal PLA operational concepts, ratified with official guidelines in 2005 and incorporated into military training and education. State-directed industrial strategies like Made in China 2025 are further operationalizations of the same thesis. The distinction between the book's formal adoption as policy and the observable behavior of the Chinese state is largely academic: the pattern of IP theft, patent exploitation, lawfare, and economic coercion documented in this testimony and elsewhere is consistent with exactly the kind of multi-domain, non-kinetic warfare the book envisioned. In their words, this is a war, not a competition.

Sun Tzu wrote that the supreme art of war is to subdue the enemy without fighting. This is the north star for the CCP. They are not competing with American companies. They are waging a campaign to acquire, replicate, and replace them—through espionage, predatory investment, coercion, lawfare, and state-subsidized competition. And because these operations do not look like war, as we know it, most Americans do not recognize the situation we are in.

The continued availability of low-cost electronics and consumer goods often masks the severity of the economic threat among the public. But those cheap goods are subsidized by the destruction of American companies and American jobs. Every solar panel sold globally with stolen American technology, every wind turbine sold with stolen American software, every telecommunications network built on stolen American R&D represents an American company

that was hollowed out, a loss of global revenue for U.S. companies, an American workforce that was displaced, and an American industry that will not easily come back.

I left government because I could no longer watch this happen from the inside. As someone who now owns a small business dedicated to countering economic espionage, I see every day how exposed Main Street is. This Committee's hearing is the first full-committee examination of CCP threats to small businesses. I commend you for convening it and thank you for the opportunity to participate.

II. The True Scale of the Threat

The most commonly cited estimate of the cost of Chinese intellectual property theft is $225 to $600 billion annually. This comes from the 2017 IP Commission report. Those numbers are dangerously incomplete.

The Commission's methodology relied heavily on counterfeit goods seized at the border and limited corporate surveys. The Commission's figures do not account for industry-level losses. When Apple effectively exits the autonomous vehicle market due in part to Chinese espionage—as former National Counterintelligence and Security Center Director Bill Evanina has publicly recounted from his conversations with Apple CEO Tim Cook—that is not a counterfeit handbag. That is the abandonment of a multi-hundred-billion-dollar industry. When Linwei Ding, a single Google engineer, walked out with the architecture for Google's Tensor Processing Unit chips—the foundation of a multi-hundred-billion-dollar AI infrastructure market—that one theft dwarfs the Commission's entire annual estimate.

The Commission's numbers do not capture cumulative technology transfer or the trickle down impact on other U.S. companies. The United States pioneered solar energy, lithium batteries, drones, wind turbine technology, advanced steel production, and the active pharmaceutical ingredients in our generic drugs. China dominates all of them today. The true scale of the threat is the systemic loss of entire industries, the adjacent sectors upon which they rely, and the downstream industries that leverage their outputs. These massive economic losses are not accounted for in customs reports.

And those numbers are eight years old. The threat has accelerated dramatically. In 2019, one in five U.S. corporations reported having been a victim of intellectual property theft. Compare this to a 2025 study in Germany that found that 87 percent of German companies have been victims of data theft, industrial espionage, or sabotage, costing the German economy nearly €300 million. FBI surveys of American companies found that China was the perpetrator in 95 percent of economic espionage cases. China is associated with more cyber espionage campaigns than any other country—30 percent more than Russia.

Trade deficits are a symptom of this problem. We will not fix trade imbalances without addressing the underlying anti-market and anti-competitive behavior that allows many Chinese

companies to undercut American businesses by selling stolen American technology at Chinese prices.

III. How China Wages This Campaign

The CCP's technology acquisition is not opportunistic. It is systematic, multi-vector, and state-directed. There are at least thirteen distinct methods the CCP uses to acquire American technology and undermine American competitiveness:

1. Forced Technology Transfer and Coerced Consent. Foreign companies seeking access to China's market are required to form joint ventures with Chinese partners, disclose proprietary technology, and manufacture locally. What begins as "consent" frequently becomes coercion. In 2018, one in five members of the American Chamber of Commerce in Shanghai reported pressure to transfer technology. Kawasaki, Siemens, Alstom, and Bombardier were all required to transfer high-speed rail technology to China; China now dominates that industry globally exporting that technology across the world.

2. Coercion Through Law. China's 2017 National Intelligence Law requires all Chinese citizens and organizations to "support, assist, and cooperate with national intelligence work." It means any Chinese national working at an American company can be compelled to cooperate with China's Ministry of State Security, with consequences for non-compliance extending to family members in China. This happens behind closed doors every day and exists as a major threat to the US workforce and our global companies.

3. Fraud. Misrepresentation as customers or licensees to gain access to technology. As an example, in around 2017, Huawei approached an Illinois based company called Akhan Semiconductor as a prospective customer to evaluate its export-controlled "Miraj Diamond Glass," and in doing so agreed not to reverse-engineer it. Huawei was reported to have retained, damaged, and transferred samples to China for analysis—triggering an FBI investigation and subsequent scrutiny. The key point is not just the incident itself, but what it represents: access was obtained legitimately, then exploited in bad faith. This highlights a fundamental issue— U.S. companies operate under a rules-based, contract-driven, profit-maximizing model, whereas some foreign competitors may operate with state alignment or strategic mandates, where acquiring technology can outweigh near-term commercial incentives. The result is a mismatch in assumptions: one side sees a customer relationship; the other may see an opportunity for capability acquisition.

4. Predatory Finance and Acquisitions. State-backed Chinese venture capital firms invest in American startups specifically to gain access to technology and talent. Oriza Ventures, a subsidiary of a Chinese state-owned investment holding company based in Suzhou, has made dozens of investments in U.S. startups. The concern extends well beyond Oriza Ventures, however. U.S. government reporting and private-sector experience suggest that some Chinese

state-linked investment activity is best understood not simply as finance, but as a means of gaining access to sensitive technology, talent, and commercial insight. In this model, venture investment, due diligence, and partnership discussions can serve as collection opportunities, allowing a counterparty to extract valuable information without ever completing a transaction. Equity investments provide more than just information, as we see below, they also provide legal standing that can be used to attack IP ownership.

5. Lawfare. The CCP weaponizes democratic legal systems against American companies. Yangtze Memory Technologies Company (YMTC)—which the Commerce Department placed on its Entity List in December 2022—filed patent infringement claims against Micron Technology. Micron alleged in its countersuit that YMTC had misappropriated Micron trade secrets; that litigation remains pending. Notably, YMTC has also pursued defamation claims against those who publicly characterize its conduct as theft—itself a form of lawfare designed to chill legitimate criticism. Separately, in the KLEO Connect dispute, Chinese investors launched dozens of lawsuits across multiple countries as part of a fight over a low earth orbit (LEO) company's spectrum rights on behalf of the PLA. As the KLEO dispute illustrates, an equity stake can do more than provide access and influence—it can also create the legal standing needed to allow an investor to use the courts to frustrate a start-ups growth.

6. Insider Espionage. Employees steal trade secrets both wittingly and unwittingly. Xiaolang Zhang and Jizhong Chen, both Apple engineers on Project Titan, stole autonomous vehicle technology. Linwei Ding stole Google's TPU designs. Xanthe and Allen Lam stole cancer drug trade secrets from the U.S. biotech firm called Genentech on behalf of a China-based biotech firm called JHL. The theft was used to convince the French pharmaceutical company, Sanofi to invest $101 million into JHL. Publicly charged cases can offer a useful window into the threat, but they cannot be relied on to represent the scale of the issue, as most incidents are not detected, not reported, and not prosecuted.

7. State-Orchestrated Talent Recruitment. More than 200 variants of talent recruitment programs—the most known being the Thousand Talents Plan—systematically recruit researchers and engineers from Western institutions. Participants maintain their American positions specifically to access and transfer IP. Harvard professor Charles Lieber received over $15 million in U.S. federal funding while secretly drawing a $50,000 monthly salary from Wuhan University of Technology under a Thousand Talents contract. He was convicted in 2021.

8. Supply Chain Infiltration. Chinese-manufactured hardware and software embedded in American networks create opportunities for surveillance, remote access, and data exfiltration without triggering a traditional cyber intrusion warning. As an example, concerns have been raised that Yealink office phones enable covert audio capture, monitoring of local network traffic, and compliance with Chinese legal terms through device service terms. TP-Link routers, whose widespread use in U.S. homes, businesses, and some government environments,

combined with repeated vulnerability findings and exposure to PRC jurisdiction, has led policymakers to warn that such devices could be exploited for espionage, network access, or facilitate cyber operations. DHS has likewise warned that Chinese-made internet-connected cameras on that U.S. critical infrastructure networks enable surveillance and exfiltration of sensitive data, with Hikvision and Dahua standing out as the best-known brand-name examples. These are the known public cases, there are many more that remain unknown to the American public, including US company products that white label these technologies under other labels.

9. Simple Theft. Physical theft of materials and prototypes. Mo Hailong dug up genetically modified corn seeds from a DuPont Pioneer test field in Iowa and tried to ship them to his employer, Beijing Dabeinong Technology Group, in China. He was caught only because a DuPont employee happened to see him in the field.

10. Cyber Intrusion. China operates the world's most expansive state-backed cyber espionage apparatus, using intrusions not only to steal intellectual property but also to map, surveil, and potentially exploit the networks on which American government, business, and critical infrastructure depend. APT41, a PRC-linked hacking group, ran years-long campaigns against more than 100 victims worldwide, including companies in defense, energy, aerospace, and healthcare, exfiltrating hundreds of gigabytes of sensitive "crown jewel" R&D, formulas, and source code. In a separate case, Chinese national Su Bin worked with PLA-linked hackers to steal sensitive military and export-controlled data from U.S. defense contractors, including designs and files related to the C-17, F-22, and F-35. More recently, the Salt Typhoon campaign showed how China's cyber operations have moved beyond corporate theft into direct penetration of U.S. telecommunications networks, where officials said PRC hackers gained access to major carriers to surveil communications, exploit lawful-intercept systems, and collect data at scale. We've caught these actors because the companies had cyber and CI resources to put towards the issue - most small companies do not.

11. Standards Manipulation. Beijing uses international standard-setting as an instrument of industrial policy, directing its firms to flood standards bodies with proposals, technical contributions, and personnel to shape competition before products ever reach the market. This matters because standards determine interoperability, compliance, and the architecture of entire technical systems; firms that influence them privilege their own technologies, raise rivals' costs, and capture licensing revenue. Huawei ranks at the top globally in 5G standard-essential patents, has submitted more than 10,000 standardization contributions, and reported about $630 million in patent licensing revenue in 2024. That means that firms building 5G-compliant products may have to license Huawei-owned intellectual property, embedding dependence even when Huawei gear is not used.

12. Data Collection via Commercial Products. This is the TikTok problem, but it extends well beyond TikTok. Chinese-developed applications and connected devices can collect behavioral, geolocation, biometric, health, and device-level data at scale, creating rich intelligence on individuals, organizations, and populations. TikTok has expressly disclosed that it may collect biometric identifiers including faceprints and voiceprints, Temu has faced legal allegations of broad sensitive-data harvesting, and connected Chinese vehicles such as those made by BYD can gather location, camera, sensor, and cabin data through modern vehicle systems. The issue is not whether a given user thinks he has "nothing to hide"; It is about whether a foreign adversary should be able to collect biometric, health, location, and behavioral data that can be used for surveillance, targeting, coercion, and operational planning.

This is not the Facebook problem of ad targeting, but the national-security problem of a foreign adversary collecting data that can be used for surveillance, coercion, identity verification, network mapping, and conflict preparation. The same logic applies to Chinese-made medical devices: in 2025, the FDA and CISA warned that Contec CMS8000 patient monitors and the relabeled Epsimed MN-120 could transmit sensitive patient data and permit unauthorized remote code execution, showing how commercial products can become collection and access points inside critical U.S. systems.

13. Intelligence Front Companies and Expert Networks. Entities that present as consulting firms, due diligence providers, or educational institutions but function as intelligence collection platforms. According to federal investigators, expert networks have charged up to $10,000 per hour for insider intelligence; one such network allegedly received $70 million in remittances for stolen secrets between 2017 and 2020. Our firm's research has identified entities operating in Silicon Valley as nonprofit "universities" with no faculty, no curriculum, and no accreditation—but with structural connections to PRC technology acquisition priorities and immigration pipelines for PRC citizens. In May 2024, President Biden issued an executive order requiring MineOne Partners Limited—a British Virgin Islands entity majority-owned by Chinese nationals—to divest property less than one mile from Francis E. Warren Air Force Base in Wyoming, home to Minuteman III intercontinental ballistic missiles. The company had established a cryptocurrency mining operation using foreign-sourced equipment in direct proximity to a cornerstone of America's nuclear triad. CFIUS learned of the operation from a public tip.

These methods work in combination. Predatory investors scout the target. Insiders extract the technology. Lawfare protects the theft. Cyber intrusions fill gaps. State subsidies scale production. And Chinese companies flood the market with products built on stolen American innovation, sold at prices no legitimate competitor can match.

IV. Why Small Businesses Are the Most Vulnerable Target

If Apple—a three-trillion-dollar company with world-class security—could not protect its autonomous vehicle program from Chinese espionage, what chance does a fifty-person startup have?

Small businesses have no security. One-third of America's small businesses rely on free, consumer-grade antivirus software. Twenty percent have no endpoint security at all. Only 17 percent conduct routine vulnerability assessments. Fewer than half use multi-factor authentication. These are not companies prepared to defend against state-sponsored cyber intrusion.

Small businesses have no legal resources. According to court filings, FemtoMetrix, a California semiconductor company, had employees steal its proprietary metrology technology and establish a competing company, Weichong Semiconductor, in China. The Chinese side hired a large international law firm specifically to bleed FemtoMetrix through legal costs. Even if FemtoMetrix prevails in court, any judgment or injunction is unenforceable in China. For a small company, the legal fight itself can be fatal.

Small businesses have no awareness. Most small business owners have never heard of talent recruitment programs, CFIUS, the 2017 Intelligence Law, supply chain surveillance risks, or the concept of instrumentalized businesses operating in their supply chain. They do not know they are targets.

Small businesses have no resilience. Sixty percent of small businesses shut down within six months of a significant cyber attack. The average cost of a cyber incident for a small business is $254,000. For a company with twenty employees, that is an extinction-level event. Only 17 percent carry cyber insurance.

Small businesses have no incentive to report. Companies do not call the FBI because they fear information sharing with regulatory agencies, public disclosure that damages their market valuation, being drawn into investigations that are incompatible with running a business, and retaliation from the PRC. The FBI documented $16.6 billion in cybercrime losses in a recent year; actual losses are estimated at 15 to 35 times that figure. The vast majority of economic espionage goes unreported.

Small businesses are the hub of innovation, the engine of the economy, and the foundation of national defense. Small businesses are 99 percent of all U.S. firms and employ nearly half the private workforce. They generate the breakthrough technologies in AI, quantum computing, and biotech that will define both economic and military superiority for a generation. They are the supply chain to the defense industrial base. Breaching a small supplier is how adversaries reach the Department of Defense. Small businesses are not peripheral targets. They are the soft underbelly of American national security and economic growth.

Small businesses are targets of predatory capital. A startup desperate for funding may not realize that its Chinese investor is backed by the state, or that the "due diligence" process is intelligence collection. Worse, taking that investment may permanently bar the company from government contracts. Under the Defense Counterintelligence and Security Agency's FOCI process, even a minority Chinese investment can render a company ineligible for facility security clearances, DoD contracts, and ITAR-controlled work. FOCI mitigation involving Chinese investors is rarely approved. Companies, such as, PatientsLikeMe and Jupiter Systems, illustrate a broader problem: startups may accept foreign capital without fully appreciating their FOCI exposure, only to discover later that the transaction carries national-security risks they cannot absorb. By then, money raised for growth must be diverted into CFIUS counsel, mitigation efforts, regulatory response, and defense costs—turning strategic investment into a drain on enterprise value before any formal divestiture occurs.

This is not only a high-technology problem. The headline cases involve AI chips and autonomous vehicles, but the CCP's interests include manufacturing processes, agricultural innovation, industrial chemistry, and consumer products. A Chinese national was caught digging up genetically modified corn seeds from a DuPont Pioneer test field in Iowa. A former DuPont employee was convicted of stealing the manufacturing process for titanium dioxide — a white pigment found in house paint, plastics, and toothpaste — and delivering it to a Chinese state-owned enterprise. A small company in Boulder, Colorado has had to remove more than 75,000 counterfeit copies of its products from online marketplaces, nearly all originating from China. If your small business makes something valuable — whether it is a semiconductor or a carabiner — you are a target. The CCP does not distinguish between critical technology and commercial technology. It takes anything that gives China a competitive or strategic advantage, and small businesses are where much of that innovation lives.

V. One Person Can Change the Future

In the intelligence world, we know that a single individual with access to the right information can alter the course of history. Oleg Penkovsky provided intelligence during the Cuban Missile Crisis that helped President Kennedy understand Khrushchev's on-the-ground capabilities, giving the U.S. side an edge. Adolf Tolkachev, a Soviet electronics engineer, provided the CIA with stealth and avionics secrets valued at billions of dollars in avoided defense R&D, giving America a generation-long air superiority advantage.

Now consider the reverse. Linwei Ding, one Google engineer, walked out with the architecture for the Tensor Processing Unit—the chips that power AI training—using nothing more sophisticated than a personal cloud account. Xiaolang Zhang, one Apple engineer, walked out with autonomous vehicle circuit board schematics. Charles Lieber, one Harvard professor, was secretly working for Wuhan University of Technology while on an American defense contract.

It took Google years and billions of dollars to develop TPU technology. It took one employee to steal it. One person inside a quantum computing startup, an AI laboratory, or a biotech company developing the next breakthrough therapy could shift the technological paradigm for a generation.

And most of the companies where these people work—especially the small ones—have zero insider threat programs, zero employee vetting, and zero access to government threat intelligence. We are leaving the vault door open.

VI. The Pattern: American Innovation, Chinese Domination

The same pattern repeats across industries. America innovates. China acquires—through theft, coercion, subsidized competition, or some combination. China dominates. American companies die or never get off the ground. And America becomes dependent on China for the very products its own innovation created—products China can restrict or withhold at will.

Solar Energy. America helped invent modern photovoltaic technology, but China captured the industry. By 2024, China held more than 80 percent of global manufacturing capacity across the core solar supply chain and more than 90 percent of some upstream segments such as polysilicon and wafers. U.S. firms including Solyndra, Evergreen Solar, and SpectraWatt collapsed as China scaled subsidized production and drove prices down, and the United States lost domestic solar wafer manufacturing altogether after 2016. What emerged was not just import dependence, but Chinese control over the industrial bottlenecks that determine cost, scale, and strategic leverage in solar energy.

Wind Turbines. American Superconductor Corporation (AMSC), a Massachusetts company, had its wind turbine control software stolen by Sinovel, a Chinese state-backed competitor. AMSC lost over a billion dollars in market value and 700 American jobs. Sinovel was fined $59 million and kept the technology. That stolen software now powers China's wind turbine industry. Chinese companies' global market share surged from 46 percent to 66 percent in a single year; Western companies collapsed from 44 percent to 22 percent. U.S. wind energy deployment now relies on supply chains that China controls, built in part on software stolen from an American company.

Telecommunications. Nortel, which went bankrupt in 2009, remains the clearest example, but it was not alone. The company endured years of cyber intrusions linked to China-based, PLA-affiliated actors, with attackers exfiltrating R&D, business plans, engineering documents, and proprietary blueprints, while Huawei rose during the same period from a marginal player to a global telecom leader. Lucent faced similar issues with insiders transferring IP to a China state supported company; and, Motorola alleged that Huawei obtained confidential base-station technology through former Motorola personnel. Taken together, these cases suggest that the decline of North American telecom champions was not a story of market competition, but one in

which sustained theft of innovation weakened incumbents while accelerating the rise of a strategic rival. Today, much of the world's telecommunications infrastructure runs on equipment from Chinese companies that rose to dominance during the same period North American competitors were drained of their IP.

Semiconductors. Micron Technology had its DRAM manufacturing process stolen by Taiwan's UMC at the direction of China's Fujian Jinhua. The estimated value of the stolen intellectual property: $400 million to $8.75 billion. UMC's fine: $60 million.

Rare Earth Materials. The United States led global rare earth production through the 1980s, with the Mountain Pass mine in California supplying approximately 70 percent of world demand. We surrendered that position through regulatory burden and strategic neglect. China used state subsidies and lax environmental standards to capture more than 90 percent of global processing. This is not a story of theft—it is a story of strategic surrender, and the consequence is that America now depends on China for materials critical to defense and advanced technology.

Pharmaceuticals. Former Genentech employees Xanthe and Allen Lam stole trade secrets for cancer drugs Rituxan, Herceptin, and Avastin and used them to defraud the French firm Sanofi into a $101 million partnership in China. Former GlaxoSmithKline biochemist Yu Xue admitted stealing company secrets for Chinese biotech firm Renopharma.

Pharmaceutical Key Starter Materials: America may discover the drug, but China increasingly controls the chemistry needed to make the drug. China is the largest foreign supplier of critical pharmaceutical inputs to the United States by volume, and its real advantage lies upstream—in key starting materials (KSM), intermediates, auxiliary chemicals, and precursor compounds that form the backbone of generic drug production. That means even medicines labeled as Indian or American likely depend on Chinese precursors for the first and most essential production steps. In practical terms, China does not need to control every finished drug; controlling the starter ingredients is often enough to control the supply chain.

The pattern is consistent and devastating. If you stand back and look at the industries China has systematically targeted—energy, communication, logistics, pharmaceuticals, advanced computing, and steel—these are the building blocks for winning in any conflict. And it is not limited to large companies or to critical technology. The same pattern plays out in agriculture, manufacturing, and consumer goods.

The strategic danger is not only lost market share, but rather in the United States moving from being the inventor to the importer — dependent on Chinese supply chains that were built, in many cases, on stolen American technology. That dependency is not an accident. It is the objective. When a country controls the supply of another nation's critical inputs, as the US has done for the past 70 years, it does not need to fire a shot to win a conflict.

VII. The Collection Infrastructure Operating in America—Funded by American Taxpayers

Beyond the headline espionage cases, an entire ecosystem of collection tools operates on American soil—much of it funded by the American taxpayer. The U.S. government subsidizes the CCP's strategic competition through at least six channels: direct research grants flowing to PRC entities, federally funded university research partnerships that produce dual-use knowledge, SBIR/STTR grants to companies with Chinese ties, pension fund capital flowing to PLA-linked corporations, the training of PRC nationals in sensitive STEM fields at taxpayer-funded institutions, and the operation of a patent system that can be weaponized against the very companies whose IP was stolen. Each channel individually has defenders who can explain why openness matters. But the cumulative picture—that American taxpayers are simultaneously funding the research, training the researchers, capitalizing the companies, granting the patents, and providing the legal system that makes it all work—is much harder to defend.

First: small business innovation grants. Senator Ernst's investigation of the SBIR and STTR programs found that six of the 25 largest SBIR/STTR awardees received nearly $180 million from the Pentagon in 2023 and 2024 despite having clear links to China—after due diligence systems were already in place. One of the companies, Triton Systems, received over $350 million in SBIR awards since 1992; its CEO had ties to CITIC Capital, a PLA-associated investment firm. He resigned in March 2025 after Congressional questioning. A 2021 internal DOD report concluded that in nearly all sampled cases, China—not the United States—was the ultimate beneficiary of DoD and other U.S. government research investments funded through SBIR. That study and subsequent congressional findings describe a recurring pattern: Chinese state-sponsored talent programs recruit key employees from SBIR-funded firms, while some recipients establish PRC subsidiaries or partnerships that shift taxpayer-funded technology toward China. Of 835 SBIR/STTR applications flagged for potential foreign influence, only 36 percent were denied. The National Institutes of Health denied all 144 applications it flagged for foreign ties; NASA denied just one out of 125.

Second: emergency relief programs. During the pandemic, between $192 and $419 million in Paycheck Protection Program loans—money designated to save American small businesses—went to Chinese-owned companies. Three companies majority-owned by Beijing's State-Owned Assets Supervision and Administration Commission settled False Claims Act allegations for $21.6 million. YAPP USA, a subsidiary of a Chinese state-owned entity, settled for $14.2 million. These were not edge cases. They were PRC government entities taking American small business relief funds.

Third: the structural vulnerability in SBA loan programs. Until March 2025, SBA's regular lending programs—the 7(a), 504, and microloan programs—required only 51 percent of a business applicant to be owned by U.S. citizens, nationals, or lawful permanent residents. The remaining 49 percent could be held by foreign investors of any nationality or immigration status.

This means that for decades, a Chinese state-obligated enterprise could have structured a U.S. subsidiary with nominal American majority ownership and qualified for taxpayer-backed SBA loans. Whether anyone exploited this gap through regular loan programs has never been investigated—and that absence of oversight is itself a scandal. The current administration has since tightened these rules, explicitly defining citizens of the PRC and Hong Kong as ineligible and requiring 100 percent U.S. citizen or national ownership. More should be done on this issue. Taxpayer-supported lending should not flow to businesses or individuals with material ties to malign state actors, and SBA should implement a formal due-diligence regime capable of identifying foreign ownership, control, influence, and other concealed risk before public funds are disbursed.

Fourth: federally funded university research. A year-long investigation by the House Select Committee on the CCP found that hundreds of millions of dollars in U.S. federal research funding over the last decade has contributed to China's technological advancements and military modernization. The investigation identified over 1,400 research publications from DOD-funded projects with Chinese partners, representing more than $2.5 billion in taxpayer funding. Over 2,000 of those DOD-funded papers included co-authors with direct ties to China's defense research and industrial base. The topics included high-performance explosives, target tracking, drone networks, nuclear physics, AI, quantum technology, and hypersonics. The National Science Foundation recovered $7.9 million from 23 grantees at 21 institutions who violated disclosure rules—all but one involved China connections. NIH flagged 540 scientists and directed 95 institutions to investigate 222 researchers; 42 percent lost their positions.

Fifth: the PhD pipeline. Approximately 723,000 Chinese nationals participated in graduate-level STEM programs at U.S. universities from 2016 through 2020, many at taxpayer-funded institutions conducting federally funded research. According to the House Select Committee, over 400 Chinese nationals at just one of six universities investigated were conducting federally funded research in sensitive fields like nuclear engineering and computer science. Every surveyed U.S. university admitted students from China's top military and defense research schools, including the "Seven Sons of National Defense." From fiscal years 2015 to 2021, federal agencies provided $28.9 million directly to Chinese entities for R&D, including DOD-funded research on technologies like drone propulsion.

Sixth: pension fund capital flowing to PLA-linked companies. U.S. investors—including banks, pension funds, foundations, insurance companies, and university endowments—have for years funded Chinese Communist Military Companies through an opaque network of subsidiaries tracked by major indexes. The House Select Committee found that BlackRock and MSCI invest or enable the investment of Americans' savings into dozens of blacklisted Chinese companies that develop weapons for the PLA. The federal Thrift Savings Plan—the retirement fund for government employees and military service members—was on track to shift billions into a China-inclusive index before lawmakers intervened. The prospect of American service

members' retirement savings funding the companies building weapons intended to be used against them should give every member of this Committee pause.

All six channels share the same structural blindness: they evaluate participants based on formal legal status—U.S. incorporation, employee headcount, ownership percentages, academic credentials—rather than functional relationship to a foreign state. The patent system itself is a seventh channel: when a Chinese entity files a U.S. patent on technology derived from stolen IP, the American taxpayer funds the patent office that examines it, and the American legal system provides the procedural protections that make challenging it expensive and slow.

Talent recruitment infrastructure. More than 200 variants of talent recruitment programs operate globally. These programs do not just recruit spies; they create a systematic pipeline for technology transfer from American institutions to Chinese ones.

Intelligence fronts and expert networks. Expert network companies are consulting firms that sell access to people, experts in their field, matching clients with industry insiders who can provide commercially valuable insight or expert testimony. Our firm has identified Chinese expert network firms that appear to serve a purpose beyond consulting, operating less like neutral research intermediaries and more like structured access platforms for acquiring sensitive commercial and technical knowledge. That is what makes the model so useful: under the appearance of routine diligence or market research, these firms can repeatedly elicit nonpublic information from individuals with privileged access while minimizing scrutiny. We have found related structures in purported nonprofit "universities" and "startup incubators" with no serious faculty, yet clear alignment with PRC technology-acquisition priorities. These entities are marketed on PRC immigration platforms as pathways for Chinese entrepreneurs to secure U.S. visas. In one case we reviewed, 65 percent of its incubator projects were led by PRC citizens, and the campus sat within a foreign-controlled real estate structure spanning Hong Kong, the Seychelles, and Ontario, a high-opacity offshore architecture consistent with concealment of beneficial ownership and strategic purpose.

Secret police and transnational repression. At least seven Chinese secret police stations have been identified operating in the United States. Two operators were arrested in Manhattan for tracking and intimidating dissidents on behalf of the Fuzhou branch of China's Ministry of Public Security. Thirty-four officers of China's MPS were charged for running thousands of fake social media accounts to harass dissidents abroad. Under Operation Fox Hunt, the PRC has forcibly repatriated more than 12,000 people from over 120 countries since 2014. FBI Director Wray has stated there are hundreds of targets on American soil. Freedom House ranks China as the world's most prolific perpetrator of transnational repression.

VIII. A Necessary Distinction: This Is the CCP, Not the Chinese People

We want to be absolutely clear about something. This fight is against the Chinese Communist Party—not against Chinese people.

Many Chinese nationals in the United States came here to escape exactly the system I am describing. They are themselves victims of CCP coercion. The 2017 Intelligence Law does not ask for volunteers; it compels cooperation and threatens consequences for refusal, including consequences for family members remaining in China. The secret police stations, the Fox Hunt operations, the social media harassment campaigns—these target Chinese diaspora communities as much as they target American institutions.

The United States is the strongest nation on earth in part because we have been a melting pot. That must not change. Operation Paperclip—the post-World War II program that brought German scientists to the United States—should be our model. We should actively facilitate the brain drain from China, welcoming talent who want to contribute to America and protecting them from CCP coercion. Any legislation we propose must include robust civil liberties protections and must target entity conduct, not ethnicity or national origin.

But we also cannot sleepwalk into obsolescence because we are afraid to name the threat. Precision is required—not silence.

IX. Why Our Legal Framework Fails Against a State-Directed Adversary

Before we turn to specific legislative proposals, this Committee needs to understand why our existing legal framework is structurally incapable of addressing the threat we have described. The problem is not that our laws are too weak in isolation. The problem is that they were designed to regulate competition between private actors operating in their own self-interest—and the PRC is not a private actor, and it is not operating in its own commercial self-interest. It is waging economic warfare.

Our courts treat PRC subsidiaries as ordinary American companies. A Huawei subsidiary incorporated in Texas receives the same procedural protections as any Texas company. A state-backed entity listed organization, YMTC, suing Micron for patent infringement is treated the same as a domestic competitor asserting a legitimate claim. Our courts do not—and under current law, cannot—account for the fact that these entities are instruments of commercial warfare, not market-based competition.

Our legal system assumes companies act in market-based self-interest. American antitrust law, patent law, trade secret law, and commercial regulation all rest on the assumption that companies are rational, market-oriented actors. They have no framework for an entity that operates at a sustained loss on purpose, files patents on stolen technology on purpose, litigates to exhaust competitors on purpose—all because it is executing a national strategy, not a revenue model. When Sinovel stole AMSC's software and then used Chinese courts to block AMSC's

enforcement, that was not commercial competition. That was lawfare—the third pillar of the PLA's Three Warfares doctrine, executed through our own legal system.

Our patent system stops at the border. U.S. patent law applies only within the United States. The ability to prohibit importation of goods incorporating infringed components is limited. A PRC entity can steal American technology, manufacture products in China using that technology, and sell those products in every market on earth except the United States—and our patent system provides no remedy. Even the International Trade Commission's Section 337 process, which can block infringing imports, is narrow, slow, and inaccessible to small businesses.

Our enforcement targets individuals, not the system. Under current law, the U.S. can prosecute the individual who stole the trade secret. But in the PRC's unified and command based economy, one company steals the technology, a second company manufactures products using it, and a third company exports those products to global markets. The theft, the production, and the market exploitation are disaggregated across separate entities—all coordinated but appearing independent to American courts. Because our system treats each entity as if it is acting independent from another, we miss the opportunity to hold the system accountable. Prosecuting the individual thief without reaching the beneficiary system is like arresting a drug dealer on the corner and missing the logistics cartel or production process.

We criminalize less serious conduct more severely. American executives go to federal prison for price fixing or engaging in anti-competitive behavior. Yet the PRC does the same thing at nation-state scale. State-subsidized dumping is coordinated price manipulation. When PRC-linked firms obtain SBIR awards, U.S. taxpayers are subsidizing Chinese innovation. The talent program apparatus is not a brain drain incentive, it's an intelligence operation. Yet we treat the American businessman as a criminal and the PRC apparatus as a trade issue. Taken together, these structural failures mean that the PRC is able to weaponize the openness of our legal system—using our procedural protections, our judicial deference, and our assumption of good-faith commercial behavior as tools of economic warfare. The legislation we propose below is designed to close these gaps.

X. What Congress Can Do

We can change this. On behalf of the 2430 Group, we would like to put several specific proposals before the Committee.

A. The Foreign Economic Espionage Organization Designation Act

Today, the entire infrastructure of Chinese economic espionage operates legally on American soil. Talent program administrators recruit insiders. Expert network operators pay thousands of dollars an hour for proprietary intelligence. Venture capital intermediaries channel state intelligence requirements through investment access. Sham universities run visa pipelines into

technology clusters. None of this is illegal unless you can prove a specific trade secret was stolen—a bar so high that the vast majority of collection activity goes unpunished.

We already have the tools to go after terrorist infrastructure. Under 18 U.S.C. §2339B, knowingly providing material support to a designated Foreign Terrorist Organization is a federal crime carrying up to twenty years. The power of that framework is that it criminalizes the infrastructure, not just the final act.

We propose creating an analogous framework for economic espionage—but targeted at the specific gap in current law. The President, on recommendation of the Director of National Intelligence, would designate specific entities as Foreign Economic Espionage Organizations, such as: named talent recruitment programs, identified expert networks functioning as intelligence collection platforms, military-civil fusion entities, and instrumentalized businesses that serve dual commercial and intelligence purposes. This targets specific programs and entities that constitute the collection infrastructure.

Here is the critical element: the criminal provision would make it unlawful for any person to **knowingly receive compensation, funding, or material benefit from a designated FEEO**. This targets the financial transaction—not association, not membership, not speech. Under current law, you cannot criminalize membership in an organization; the Supreme Court settled this in *Holder v. Humanitarian Law Project* (2010).

This would mean that a talent participant, like Charles Lieber, drawing a $50,000 monthly salary from a PLA-affiliated university while working at an American research lab, could be prosecuted. This gives companies the hook they need to terminate employment, when they recognize talent membership among their employees. The startup founder whose “investment” from a state-linked fund comes with undisclosed reporting obligations. The visa pipeline business that draws compensation in order to place PRC citizens in American technology companies. Right now, unless you can prove these people stole a specific trade secret, there is no crime. Under this Act, the government only needs to prove two things: the entity is designated, and the defendant knowingly accepted compensation from it.

Penalties would be comparable to material support for terrorism—up to fifteen years. The Act would include a knowledge requirement: you must know, or be willfully blind to the fact, that the entity is designated. This protects innocent commercial transactions. And critically, it would include an affirmative defense for individuals who report coercion and cooperate with law enforcement. A Chinese researcher being pressured under the 2017 Intelligence Law should have an off-ramp—report the coercion, cooperate, and receive protection rather than prosecution. This is Operation Paperclip with a legal framework.

B. The Malign Foreign Interests Disclosure Act

American small businesses cannot protect themselves from threats they cannot see. Today, a small company purchasing a VOIP phone system has no way to know it is buying a collection platform. A startup accepting a venture capital term sheet has no way to know the money is state capital with intelligence requirements attached.

We propose requiring disclosure by any entity operating in the United States that has received material support from a country of concern, whether directly or indirectly, including through: (1) equity investment by a state-owned, state-controlled, or state-directed entity, or by any subsidiary, affiliate, or intermediary acting on its behalf; (2) loans, grants, subsidies, or other financial assistance from a foreign government or state-linked institution, including through offshore shell companies or similar pass-through structures; (3) participation by any officer, director, or key employee in a foreign government talent-recruitment program; (4) technology-licensing, technology-transfer, or joint-development agreements with state-linked entities; or (5) any contractual, statutory, or informal obligation to provide data, technology, research, or intelligence to a foreign government or its affiliates.

The threshold is not an ownership percentage, as they are easily circumvented through layered corporate structures or routed through offshore jurisdictions. The threshold is any material state support. Disclosures would go to a public registry housed at the Department of Commerce, searchable by any American business considering a vendor, investor, or partner.

This is not about criminalizing foreign investment. Companies that disclose their connections and operate lawfully have nothing to fear. But American businesses deserve to know who they are doing business with.

C. The Economic Espionage Infrastructure Act

The Economic Espionage Act must be strengthened to target the beneficiaries of trade secret theft, not just the individual thieves. In the AMSC case, Sinovel canceled nearly $800 million in contracts when it stole AMSC's software, then generated billions in revenue from that stolen technology. Its punishment: a $59 million fine. Sinovel kept the technology. The fine was less than the cost of developing the software legitimately. Stealing was a rational economic decision.

The PRC's unified economy means one company can steal intellectual property and an entirely different company can benefit from it—with no formal legal connection between the two. The statute must be broadened to allow prosecution of any party that uses, benefits from, or facilitates the use of stolen technology, with penalties severe enough to change the economic calculus. As it stands, prosecuting individuals without devastating the beneficiary system is like arresting drug dealers while leaving the cartel untouched.

D. Patent and IP Enforcement Reform

Our patent system was not designed for an adversary that steals technology, patents it, and then uses those patents offensively against the original inventor. We propose two reforms. First, allow the Patent Trial and Appeal Board to review trade secret evidence and provide in-camera review by default, so companies can challenge patents built on stolen innovation through the most cost-effective mechanism available. Second, once a U.S. court or the International Trade Commission makes a trade secret misappropriation finding involving entities linked to a country of concern, the PTO should institute enhanced prior art and provenance review for patent applications in the same technology area from entities connected to the theft. This is not blocking patent filings based on national origin—it is applying heightened scrutiny where a specific theft has already been proven, the same logic that underlies enhanced CFIUS review.

E. Proposals Within This Committee's Jurisdiction

Small Business Economic Defense Act. Authorize the SBA to establish a dedicated counter-economic espionage program delivered through Small Business Development Centers. This would include threat briefings, counterintelligence assessments, and incident response for small businesses. The current SBA cybersecurity budget is $3 million nationally. That is not a serious response to a multi-hundred-billion-dollar threat that occurs through non-cyber means.

SBIR/STTR Security Enhancement. Strengthen national security screening across all twelve participating agencies, building on the Senate's S. 3971. Mandate screening for foreign government talent program participation. When 36 percent of reviewed applications are denied for foreign adversary concerns, and only one of twelve agencies is meaningfully screening, the program is being exploited.

Small Business Cybersecurity Investment Act. A 30 percent tax credit, up to $75,000 annually, for cybersecurity investments by firms under 250 employees. This should cover hardware, software, training, assessments, and dedicated security personnel.

Small Business IP Legal Defense Fund. A federal fund covering up to $250,000 in legal costs for small businesses fighting intellectual property theft by state-sponsored actors. Small businesses cannot afford international IP litigation; this fund levels the playing field.

Small Business Threat Intelligence Program. Direct CISA and the FBI to provide actionable, declassified threat intelligence specifically tailored for small businesses, delivered through SBA channels. Today, classified threat briefings reach Fortune 500 companies but never reach Main Street. That must change.

Counter-Espionage Subsidies and Tax Credits. We do not ask American citizens to wage war against foreign nation states. That is the responsibility of the national government. But right now, that is exactly what we are asking small businesses to do—defend themselves against a state-directed intelligence campaign with no tools, no training, and no support. As the CCP calls this warfare, the U.S. government has an obligation to provide the resources for small businesses

to establish counterintelligence programs, the same way we fund national defense. This should include direct subsidies or matching grants for small businesses to establish CI programs, in addition to tax credits for investments in counterintelligence, employee vetting, and security training.

Some state laws currently prevent companies from conducting due diligence on employees—California's Investigative Consumer Reporting Agencies Act, for example, limits companies' ability to investigate whether employees participate in foreign talent programs. Companies working on critical technology need both the federal authority and the financial incentive to know who their people are.

F. Additional Cross-Committee Recommendations

Whistleblower Bounty Program. Modeled on the Dodd-Frank SEC program, paired with immigration benefits for foreign national whistleblowers who report economic espionage. Create a proactive incentive for people to come forward.

Qui Tam Enforcement Model. When a company identifies and reports state-sponsored trade secret theft, DOJ takes the lead on prosecution so the company does not bear the legal cost. When the case results in penalties, the reporting company shares in the financial recovery. This changes the fiduciary calculus from silence to action.

Federal Preemption of Obstructive State Privacy Laws. Provide federal authority for companies working on critical technology to conduct employee due diligence, overriding state laws that currently prevent it.

Predatory Capital Disclosure Requirements. Require venture capital firms to disclose foreign government investor connections to portfolio companies and to CFIUS.

Chinese Whistleblower and Defector Protection. Create immigration and protection pathways for Chinese nationals who report CCP economic espionage operations. This facilitates the brain drain while protecting individuals from retaliation.

XI. Conclusion

American industries are being hollowed out. American technology is being illicitly acquired and turned against us. American small businesses—99 percent of all U.S. firms, employing nearly half the private workforce—are on the front lines with no defenses, no intelligence, and no support.

The measures we have proposed are achievable. Our allies face the same threats from the same actors, and some have developed legislative approaches worth studying. This should be an international effort as well as a domestic one.

But the essential point is this: if this is a war—and if we listen to PLA doctrine it is —then Main Street should not have to fight it alone. With the right framework, it will not have to.

Thank you. I welcome the Committee's questions.