Written Testimony

Before the Senate Judiciary Committee

"Stealth Stealing: China's Ongoing Theft of U.S. Innovation"

Tom Lyons
Co-Founder, The 2430 Group
April 2026

I. Introduction

Chairman Grassley, Ranking Member Durbin, and Members of the Committee — thank you for the opportunity to testify on China's ongoing theft of American innovation. My name is Tom Lyons. I am the co-founder of the 2430 Group, a nonpartisan organization focused on countering economic espionage.

I spent a career at CIA focused on foreign adversary capabilities and intentions, not intellectual property theft. But you cannot work in the intelligence community without seeing the evidence of China's economic espionage throughout the United States: front companies operating freely, talent programs strip-mining our high-tech companies, and core infrastructure built upon stolen American trade secrets. The magnitude of China's effort was staggering. The response — from both the private sector and government — was not.

After leaving government, our team took on a mission we could not have pursued from the inside, that is partnering with U.S. companies and universities to help them defend their innovations. What we have found has been alarming. This written testimony highlights why our current framework is failing our needs and proposes specific legislative measures this Committee can enact to address the threat.

Case Studies

The following cases are not chosen because they are exceptions to the rule. They are chosen because they are representative of the norm. Each illustrates a different facet of how China's system operates — insider recruitment, cyber intrusion, state-backed litigation, and systematic talent program exploitation — and each demonstrates the same outcome: the individual is prosecuted, the system is untouched, and the industry migrates.

American Superconductor (AMSC). A Devens, Massachusetts company that developed proprietary wind turbine control software. Its largest customer was Sinovel, a Chinese state-backed enterprise that accounted for over seventy percent of AMSC's revenue. In 2011, Sinovel recruited an AMSC employee to hand over the source code. Overnight, Sinovel stopped accepting shipments, stopped returning calls, and stopped paying. AMSC lost over a billion dollars in market value and went from more than nine hundred employees to under three hundred. Sinovel was prosecuted by DOJ, convicted, and fined $59 million, all the while continuing to manufacture turbines using the stolen

software. That software now helps power China's globally dominant wind turbine industry. AMSC, meanwhile, funded its own civil litigation across multiple jurisdictions, for years, while hemorrhaging revenue and fighting for survival — competing against its own products.

Nortel Networks. Once North America's most valuable technology company. PLA-linked hackers penetrated Nortel's systems and maintained access for nearly a decade, exfiltrating R&D plans, engineering designs, product roadmaps, and business strategy. During that exact period, Huawei rose from a marginal player to a global telecommunications leader. Nortel filed for bankruptcy in 2009. Today, Huawei holds 31 percent of the global telecom equipment market. Ericsson holds 13 percent. Nokia holds 14 percent. No American company holds a meaningful share.

Linwei Ding and Google. Linwei Ding, a Google engineer, was found guilty on fourteen counts of economic espionage and trade secret theft for stealing over two thousand pages of trade secrets, including the designs for Google's sixth-generation Tensor Processing Unit — technology at the center of a trillion-dollar industry. What is most striking about Ding is not the theft itself. It is that he advertised the stolen designs as his company's differentiator when he was in the PRC. He pitched them openly to investors. The theft was a credential. When a system reaches the point where stolen intellectual property is a qualification for venture funding, you are not dealing with rogue actors. We are dealing with a system. And while Ding was caught, the technology is gone. We will see the consequences in several years through low-cost, state-subsidized PRC products built on American innovation.

Apple's Autonomous Vehicle Program. Apple's autonomous vehicle program was hit by three separate major PRC theft cases. DOJ prosecuted the individuals involved but not the companies that commissioned the theft or the system that incentivized the behavior. Today, Apple has abandoned its autonomous vehicle program, in part due to this espionage (as recounted in the book, *The Great Heist*), while the PRC autonomous vehicle industry is the fastest growing on the planet. The pattern is unmistakable: the technology is stolen, the individual is prosecuted, the system is untouched, and the industry migrates.

These are not isolated incidents. They are the output of a strategy. In solar energy, China now holds eighty percent of a market that American and European companies developed. In telecom, after Lucent and Nortel were hollowed out, the United States lost

its global position entirely. In high-speed rail, commercial drones, EV batteries, port cranes, and pharmaceutical ingredients, the same trajectory has played out. An industry is targeted. Its technology is acquired. State subsidies crash the price. The original innovators are driven from the market.

II. The Corporate Disconnect

American firms are not competing against Chinese rivals in any normal sense. They are competing against the largest intelligence apparatus in the world — one whose mission includes putting American companies out of business. This is not GM versus Ford. This is a U.S. startup versus the PLA. This is a breakthrough battery company versus the full resources of the second-largest economy on the planet.

Our commercial and legal systems were never designed for this type of adversary. Our companies assume good-faith, self-interested actors, who will abide by non-disclosure agreements. Our courts assume that parties to a dispute share a basic commitment to honest dealing. Our regulatory frameworks assume that companies are motivated by profit and operate independently. These are reasonable assumptions in a market economy. They are flatly wrong when applied to entities that operate under the direction and receive support from a party-state that compels theft, incentivizes copycat products, subsidizes product offerings – profit is irrelevant.

Today, American companies are defending themselves against the Ministry of State Security, but treating it like a compliance issue. And those who should care most — the C-suite — typically don't. This is because their worlds are dominated by quarterly earnings and near-term revenue, whereas espionage can be a five year problem.

More specifically, just as the timeline from initial targeting of a U.S. company to the successful theft of its technology can unfold over years, the timeline from the theft to the commercialization of the stolen technology, can take still more time. Then, from the period of commercialization to when an American company feels the competitive impact, in the form of lost contracts, eroded margins, or a foreign competitor that appeared from nowhere with an identical product, years may have passed. As such, the cycle of economic espionage is measured over years, which creates an illusion that the threat is not immediate. Consequently, a CEO looking at this quarter's earnings sees no emergency. By the time the damage is visible in a balance sheet, the theft happened

years ago, the technology has been fully absorbed, and the window to respond has closed.

Given this reality, counterintelligence products and services are often viewed as a cost center by companies versus an opportunity to protect long-term revenue. Furthermore, even if theft is detected, there are two main reasons why companies do not pursue cases.

Under the current system, the company that was robbed must detect the espionage, investigate it, report it, and cooperate with prosecution — all while absorbing the financial and competitive losses and facing the prospect of PRC retaliation. The retaliation is real and can be devastating: companies risk losing market access, facing regulatory targeting, or suffering supply chain disruption.

For small and mid-size companies, the financial burden of detection and litigation is insurmountable. Public companies frequently choose silence because disclosure damages market valuation or invites questions into the management of the company. The result is that most economic espionage is never reported, let alone prosecuted.

Companies also remain silent due to the specific accounting standard that governs how those losses are reported, which unintentionally renders economic espionage invisible. Under the Accounting Standard Codification of the U.S. Generally Accepted Accounting Principles 450-20 (ASC 450-20) companies are required to disclose loss contingencies that are *probable and estimable*. Losses from IP theft rarely meet this threshold. This is because it requires companies to quantify the loss based on an estimation of the future value of stolen technology in a competitor's hands. This calculation most often falls into the "not estimable" category and the result is that trade secret theft losses are structurally invisible in corporate financial statements. The scale of the problem is hidden not by intent but by accounting standards that were never designed to capture it.

The effect of these realities is that both the government and private sector are ill-informed on the volume and impact of economic espionage that occurs daily, because there is no requirement to report it and thus zero market consequence for losing trade secrets or IP.

Ultimately, these disconnects are causing U.S. companies to miss or misread signals around their competitive advantages and thus remain complacent. Just as the U.S. silently watched wholesale industries, such as the solar, battery, port infrastructure, steel, and telecom equipment industries transfer to the PRC, if we do not change the

paradigm, continued loss of industry will impair the future US economic development and ultimately, the US freedom of action. The corporate realities are compounded by a legal framework that is equally mismatched.

III. The Legal Disconnect

The legal framework governing economic espionage in the United States was built for a world that no longer exists. It assumes that theft is committed by identifiable individuals, that victims know they have been robbed, that civil courts can provide meaningful remedies, or that the support structure is illicit. However, none of these assumptions hold against a state-sponsored adversary. The result is a series of disconnects between the threat and the tools available to address it, which leaves American companies exposed at every stage: before the theft, during the theft, and after the theft.

Before the theft even occurs, American companies operate blind. There is no legal requirement for foreign entities to disclose state backing, intelligence obligations, or participation in government talent-recruitment programs. A small U.S. manufacturer evaluating a PRC investment partner has no way to know the capital carries intelligence requirements. A university hiring a visiting researcher has no way to know the researcher's sponsoring institution is contracted by the MSS. A technology company onboarding a new employee has no way to know that employee is drawing a second salary from a PLA-affiliated program. Meanwhile, the entire apparatus that enables the theft, such as talent recruitment hubs, the front companies, the expert networks, the state-backed venture funds, all operate legally on American soil. A talent program administrator can recruit an insider, an expert network can pay thousands of dollars for proprietary intelligence, and a venture capital intermediary can channel state intelligence requirements through investment due diligence, and none of it is a crime. We only criminalize the final act — the moment a trade secret is taken. Everything upstream of that moment, the entire infrastructure that makes the theft inevitable, is legal.

Once the theft occurs, the legal response is equally mismatched. The Economic Espionage Act provides criminal penalties, but DOJ brings only ten to twenty cases a year against the thousands of incidents occurring. And importantly, the fines are a fraction of the value stolen, making the penalty worth the risk and the victim company receives nothing from the prosecution. While civil remedies under the Defend Trade

Secrets Act are theoretically available, they are practically useless against Chinese state-backed entities because judgments are unenforceable against defendants with no U.S. assets, legal discovery in China is impossible, and litigation costs millions over years with near-zero recovery. As such, companies that commercialize the stolen technology, the investors that funded the operation, the entities that file patents on the stolen IP — the beneficiaries — face no consequences at all. The individual thief may be prosecuted. The system that directed the theft, financed it, and profited from it remains untouched.

Perhaps the clearest illustration of the structural mismatch in our legal system is what happened to Micron Technology. Micron had its DRAM manufacturing process stolen when employees illicitly transferred Micron's proprietary technology to Fujian Jinhua, a Chinese state-backed chipmaker that the Commerce Department placed on its Entity List. Micron estimated its losses up to $8.75 billion. The criminal fine against UMC: $60 million.

Then, separately, Yangtze Memory Technologies Company (YMTC), a Chinese state-owned memory chipmaker also placed on the Entity List and identified by the Pentagon as a military-affiliated company, sued Micron for patent infringement in U.S. federal court. Micron's defense was that YMTC had stolen and patented Micron's own trade secrets, and that YMTC's patents should be invalidated due to misappropriation. And yet in discovery, a federal court ordered Micron to hand over seventy-three pages of printed source code, the substantive core of its most advanced chip design.

Micron fought the order to the Federal Circuit, arguing the court had ignored national security concerns and the Executive Branch's own designation of YMTC as a threat. The Federal Circuit denied the petition. Micron petitioned the Supreme Court, arguing that once paper copies leave a controlled environment, the damage can never be undone. Micron lost.

Consider what this means: a sanctioned Chinese entity, designated by our own government as a national security risk, used our civil discovery system to compel an American company to surrender its most closely held source code and our courts enforced the theft.

Compare the Micron case with how China treats American companies. China can ban a company from its entire market overnight, with no evidence, no process, and no appeal. The NBA lost hundreds of millions in revenue over a single tweet. H&M was effectively

expelled from the PRC market for raising concerns about Xinjiang. Australia saw its wine exports to China destroyed overnight after calling for a COVID-19 origin investigation.

Furthermore, when the Department of Defense designated Chinese companies with military ties under Section 1260H of the FY2021 NDAA, companies like Xiaomi challenged those designations in U.S. court and won because DoD could not produce sufficient *unclassified* evidence. China bans companies with no evidence; the United States cannot even maintain its own designations.

The asymmetry extends to the operating environment. American companies in China face forced joint ventures, mandatory technology transfer, source code disclosure, and CCP party committees embedded in every major private company — 1.6 million party cells, with 100 percent coverage of the top 500 firms. Chinese entities operating in the United States face no reciprocal obligations.

IV. Why Participation Is Rational

The scale of China's economic espionage cannot be explained by the actions of rogue individuals. It can only be explained by a system that has made participation rational for every actor within it.

The PRC has made technology acquisition a national priority through formal state plans, such as the Made in China 2025 Program. It has allocated funding and infrastructure to ensure that participation in its system is financially lucrative, professionally prestigious, and legally compulsory. Talent programs offer signing bonuses of half a million dollars or more, plus housing, lab space, and equity participation. Recruits into the programs are celebrated as national heroes. And, due to the PRC 2017 National Intelligence Law, PRC citizens face imprisonment if they do not cooperate with the PRC government requests.

Given the lack of incentive in the U.S. corporate sector to invest in counterespionage resources, let alone prosecute espionage, the probability of successfully executing economic espionage is high. Furthermore, given that the penalties in the U.S. are a fraction of the value of what was stolen and the professional and financial rewards for success are enormous, for any rational actor, the calculus is clear. The expected return on espionage overwhelmingly favors acquisition over independent innovation.

This is why case-by-case prosecution cannot solve the problem. You cannot deter what a system incentivizes. When millions of individual actors face the same risk-reward calculation, the only effective response is to change the system-level incentives — by making the infrastructure illegal, the consequences devastating, and the rewards for reporting greater than the rewards for silence.

V. An International Problem Requiring an Allied Response

This is not a problem unique to the United States. Every advanced economy faces the same threat. The European Union, the United Kingdom, Australia, Canada, Japan, South Korea, and Taiwan have all experienced systematic Chinese state-sponsored economic espionage targeting their most critical industries. Our allies are developing their own responses — the EU's Foreign Subsidies Regulation, Australia's foreign influence transparency scheme, the UK's National Security and Investment Act — but these efforts remain fragmented. The United States should lead a coordinated allied framework for mutual defense against economic espionage: shared intelligence on targeting patterns, harmonized designation and sanctions regimes, joint import exclusion mechanisms, and reciprocal enforcement of trade secret judgments. China's strategy depends on exploiting each country individually. A unified allied response would fundamentally change that calculus.

VI. Legislative Proposals

The following proposals are designed to address the structural failures described above. Each is calibrated to this Committee's jurisdiction and builds on existing legislative models with proven track records.

1. Qui Tam Enforcement Model for Economic Espionage

DOJ already has the authority to prosecute economic espionage under the EEA. The problem is that companies have no incentive to report. Under the current system, a company that reports theft cooperates with a multi-year investigation, bears the cost and disruption of that cooperation, risks PRC retaliation, and receives nothing. The fines go to Treasury. The company is left to pursue its own civil remedies under the DTSA — at a cost of millions, with near-zero chance of collecting from entities in China.

We propose a qui tam model, adapted from the False Claims Act. Under this model, a company that reports state-sponsored trade secret theft to DOJ through a confidential

channel would share in the financial recovery — criminal fines, forfeitures, and sanctions penalties. A confidential investigative window of 12 to 18 months would protect reporting companies from premature disclosure and retaliation. DOJ would bring the full resources of the FBI, NSA, and ODNI to the investigation; resources no private company can access.

This transforms the economics of reporting. Instead of bearing cost for no return, companies receive a financial incentive to come forward. The government gets cases it would never otherwise hear about. The reporting company gets recovery it could never achieve through civil litigation.

2. Whistleblower Bounty Program

Whereas qui tam brings companies forward, this incentivizes individuals with knowledge of theft to come forward. Modeled on the Dodd-Frank SEC whistleblower program, this would provide financial bounties or immigration benefits to individuals in talent programs, employees at front companies, or participants in acquisition networks. Giving them a protected pathway to come forward is essential for getting ahead of the issue.

3. Expand EEA to Cover Beneficiaries and Infrastructure

The EEA currently targets the individual who stole and, in some cases, the entity that directed the theft. The broader ecosystem of beneficiaries, such as the companies that commercialize stolen technology, the investors that funded the operation, the entities that file patents on stolen IP, often face no consequences.

We propose expanding criminal liability to entities that knowingly benefit from trade secrets acquired through economic espionage. When DOJ establishes that an entity benefited from state-sponsored theft, a cascade of consequences should trigger automatically: Entity List designation, import exclusion, patent system sanctions, financial system restrictions, and government procurement bans. The entity can be de-listed by ceasing use, paying restitution, and accepting compliance monitoring.

Additionally, we propose that the Department of Commerce be given the authority to ban the import of any product, in whole or in part, made with intellectual property determined to have been stolen from a U.S. company. This would mirror existing authorities for goods produced with forced labor and would ensure that stolen American innovation cannot be commercialized back into our own market. An import ban changes

the calculus for every company in the supply chain — if a component was made with stolen IP, the entire product is excluded.

4. Foreign Economic Espionage Designation Act

Today, the entire infrastructure of Chinese economic espionage operates legally on American soil. Talent program administrators recruit insiders. Expert networks pay thousands 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 Executive, 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 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.

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 needed to terminate employment, when they recognize talent membership among their employees. 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 or material benefit from it.

A Chinese researcher being pressured under the 2017 Intelligence Law should have an off-ramp to report the coercion, cooperate, and receive protection rather than prosecution. This is Operation Paperclip with a legal framework.

5. The Malign Foreign Interests Disclosure Act

American small businesses cannot protect themselves from threats they cannot see. Today, a small company purchasing an inexpensive VOIP phone system has no way to know it is buying a PRC 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 and whether it is a nonmarket-oriented partner.

6. Patent Law Reform

PRC entities steal American trade secrets, patent the resulting technology, and then weaponize those patents against the original innovators. Current law provides no

adequate remedy. Inter partes review at the PTAB does not allow trade secret evidence. Derivation proceedings have a one-year filing window that is practically useless in the China context. Federal court litigation takes three to five years and costs $3 to $10 million.

We propose a three-part reform:

Prove It: Enable companies to internally document and timestamp their trade secrets through a verified, commercially available timestamping technology — so that ownership and the date of creation can be established with legal certainty in any subsequent proceeding.

Challenge It: Create a fast-track PTAB proceeding to challenge patents derived from stolen trade secrets. Unlike existing proceedings, this would allow trade secret evidence to be reviewed in camera by default to protect remaining secrets, shift the burden to the patent holder to prove independent development, and carry a twelve-month resolution timeline.

Punish It: When a foreign entity is found to have benefited from stolen American trade secrets, mandatory consequences follow automatically: Entity List designation, import exclusion, patent system sanctions, financial system exclusion, and government procurement ban.

7. Mandatory Counterintelligence Assessments

We propose mandatory counterintelligence assessments and foreign influence background checks for every federal contractor and grant recipient. Additionally, companies, particularly in the tech sector, must be given federal authority to conduct foreign ownership, control, or influence (FOCI) checks on employees.

8. Federal Preemption of State Laws that Prevent FOCI Checks

Some state employment and privacy laws, such as California's Investigative Consumer Reporting Agencies Act (ICRAA), Civil Code §1786 et seq., regulate background checks for employment, tenant screening, and insurance. It requires employers/landlords to provide written disclosure, obtain consent, and allow applicants to receive a copy of completed reports. In effect, this state law prevents companies from conducting these assessments, as a counterintelligence assessment is not something that should be shared

with the employment candidate. Congress can preempt this statute, allowing technology companies the federal authority to conduct FOCI checks.

9. Tax Credits for Counter-Espionage Programs

Detection is upstream of everything. Companies cannot file qui tam reports if they never discover the theft. Insider threat monitoring, trade secret inventories, network anomaly detection, and foreign travel policies are pure cost centers today with no revenue upside. A tax credit covering a meaningful share of qualified counter-espionage expenditures would give security teams the ability to win internal budget fights against executives focused on quarterly returns. The federal government gets an enormous return: companies with counter-espionage programs detect earlier, preserve better evidence, and produce stronger cases. The tax credit feeds the qui tam pipeline.

The credit should cover 30 to 50 percent of qualified counter-espionage expenditures, defined to include at least, insider threat detection and monitoring systems, network anomaly detection and data loss prevention tools, counterintelligence training for employees with access to proprietary technology, foreign travel security protocols and device management, and third-party security audits focused on state-sponsored threat vectors. Eligibility should be tiered to where companies below $500 million in revenue get the full credit; larger companies get a reduced rate but can claim it against a broader base of expenditures. To prevent abuse, qualifying expenditures would need to be certified against accepted standards certified by CISA.

10. Federally-Backed Insurance for Trade Secret Theft

Modeled on the Terrorism Risk Insurance Act (TRIA), this would create a federally-backed insurance program for trade secret theft by foreign state actors. Companies that maintain adequate counter-espionage programs would be eligible for coverage to insure their commercial losses due to theft and market losses. This would have the effect of shifting the calculus from silence to action.

The TRIA model works because it solved a specific market failure: after 9/11, private insurers could not price catastrophic terrorism risk, so they stopped writing policies, which left the entire commercial real estate market uninsurable. The same market failure exists for state-sponsored IP theft; no actuary can model the probability that the PRC will target a specific company's trade secrets, so the coverage doesn't exist. Under this proposal, the federal government would serve as the backstop reinsurer above a

defined loss threshold. Private insurers would underwrite the policies and set premiums. Eligibility would be conditional on maintaining a qualifying counter-espionage program. Insurers would audit security practices: companies with strong programs get lower premiums, companies with weak programs pay more or are denied coverage. Claims would be triggered by a federal finding, such as an EEA prosecution, a Commerce Department finding, or a qui tam recovery establishing that state-sponsored theft occurred. The critical behavioral shift is that insured companies have less reason to stay silent and more reason to act.

VII. A Critical Distinction: The CCP and the Chinese People

It is essential that any legislative response target the party-state apparatus, not the Chinese people. Chinese nationals are often the first victims of this system — coerced into participation through legal compulsion, family pressure, and exit bans. Researchers recruited through talent programs frequently do not know that the sponsoring organization is contracted by the Chinese government. The recruitment arrives as a professional opportunity — a conference invitation, a visiting scholar offer, a collaboration proposal — through organizations that appear entirely legitimate.

The whistleblower protections and immigration benefits proposed in this testimony are specifically designed to protect individuals caught in this system and to give them a pathway out. America's ability to attract and integrate global talent — including Chinese talent — remains one of our most decisive competitive advantages. Protecting that advantage requires targeting the system that exploits these individuals, not the individuals themselves.

VIII. Consequences of Inaction

Today, the United States runs a trade surplus in intellectual property licensing — we earn more from the world using our innovations than we pay to use anyone else's. That surplus is the economic dividend of seventy-five years of American investment in research, education, and institutional trust. It is the foundation of our economic power. And it is being dismantled, industry by industry.

If this trajectory continues, the United States faces the same decline that Britain experienced after losing its industrial supremacy — a former great power that still carries influence but no longer sets the terms. Britain did not collapse overnight. It was overtaken gradually, as the industries it pioneered were mastered and scaled by

competitors who studied its innovations and outproduced it. The parallels are not subtle.

Unlike Britain, we face a competitor that is not outcompeting us. It is systematically stealing the foundations of our advantage while building the capacity to deny us freedom of action. Every stolen technology strengthens China's military-industrial base. Every PRC-manufactured product embedded in American infrastructure extends Beijing's intelligence reach. Every industry that migrates weakens the innovation base that sustains American economic and military power.

IX. Conclusion

If a foreign military were conducting operations against American companies on American soil, we would not ask those companies to fund their own defense. But that is the current reality. The PRC's intelligence services are targeting our firms, our labs, and our people — and we have outsourced the response to compliance departments and general counsel.

In the PRC system, while an individual may steal the technology, they do it on behalf of a system that nationally prioritizes the behavior. In the United States, we address neither the infrastructure that incites the theft nor the companies that benefit from it. Our occasional convictions do not un-steal the technology that proliferates and destroys our industries.

The proposals in this testimony are achievable measures. 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: our private and academic sectors should not have to fight a nation-state alone. With the right framework, they will not have to.

Thank you. I look forward to the Committee's questions.