INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

JUNE 2025

Countering Insider Theft of National Security Technology

Presented by

INSA'S INSIDER THREAT SUBCOMMITTEE

Building a Stronger Intelligence Community

EXECUTIVE SUMMARY

The wholesale theft of national security technologies by foreign adversaries poses a significant threat to the long-term security of the United States. American organizations developing cutting-edge dual-use technologies, such as artificial intelligence (AI) and quantum computing, are aggressively targeted by actors seeking to steal intellectual property. These efforts focus on government and commercial employees, contractors, foreign visa holders, and academics.

Given the increasing efforts by nation-states to acquire U.S. national security technologies, swift and decisive action is required to counter this existential threat.

This threat vector aligns with insider threat concerns. While the U.S. government addresses such risks within classified environments through measures like Executive Order 13587 and the National Industrial Security Program Operating Manual (NISPOM), many emerging technologies with national security implications are developed in smaller companies and academic institutions. These environments foster open collaboration and encourage publication and patenting of advancements. While these practices benefit innovation, they leave organizations vulnerable to foreign insider exploitation due to limited awareness and resources.

Foreign adversaries, particularly the Chinese Communist Party (CCP), have long recognized this "Achilles heel" and exploit it through cyber and human espionage, economic coercion, and manipulation of academic and business partnerships. As U.S. cyber and technical defenses have strengthened over the last decade, adversaries have increasingly turned to human-enabled intellectual property theft. This includes subtle recruitment of company employees, contractors, students, researchers, and academics,[1] as well as the placement of their own collectors into targeted companies and university programs (i.e., seeding operations). This rapid and sophisticated campaign is accelerating. Based on recent congressional testimony by The Hon. Bill Evanina, Michael Pillsbury, and Craig Singleton, these efforts will only intensify.[2]

This paper identifies critical gaps in current defenses and provides actionable recommendations to begin closing them.

INTRODUCTION

The theft of American national security technology has long been of grave concern for U.S. government leaders and the Intelligence and National Security Alliance (INSA). This paper serves as an update to INSA's May 2021 publication, 'Insider Threats and Commercial Espionage: Economic and National Security Impacts'.[3]

While many observations and recommendations from the 2021 paper remain relevant, the past four years have brought significant changes in three key areas:

- **The accelerated advancement of critical national security technologies.** Experts widely agree that foreign dominance in fields such as AI, biogenetics, and quantum computing would profoundly impact U.S. national security and global power competition. The pace of development in these transformative technologies is surpassing even the most optimistic expectations.
- **The expanded use of commercial, public, and stolen data to target individuals.** The CCP, for example, has infiltrated government and commercial databases to amass personal, financial, medical, legal, criminal and social media data. CCP operations such as Salt Typhoon (targeting private sector telecommunications companies) and Volt Typhoon (targeting U.S. critical infrastructure) are prime examples of their continued nefarious activities in the cyber domain. This information supports counterintelligence operations and the targeting of individuals who can grant access for espionage or enable offensive and gray zone activities.
- **Intensifying global superpower competition.** China's slowing economic growth, growing assertiveness in the South China Sea and increasing pressure on Taiwan, and an escalating U.S.-China trade war have heightened tensions. This rivalry has led to a surge in CCP efforts to steal American technological advancements.

America's strength is rooted in its intellectual capital and enduring drive to iterate, expand, and invent, whether through medical breakthroughs, technological discoveries, quality of life improvements, or national security solutions. These advancements often originate in academic/research institutions or small startups.

However, foreign adversaries routinely exploit America's open culture, especially within universities and small companies. Institutions conducting cutting-edge research on dual-use technologies and processes or government-sponsored research face growing insider theft risks. Some foreign scholars, aligned with adversarial nations, misappropriate American research and emerging technologies, secure patents or production rights abroad, and sell these items back into the U.S. market—undermining the very universities and businesses that developed them.

The challenge for academic and private organizations outside the cleared space is often a lack of risk awareness. Many do not recognize the severity of this threat to both national security and their own competitive advantage. They may not consider themselves a target, focusing instead on their work and assuming everyone involved shares a mutual commitment to success. Even among those who are aware of the risk, few possess the resources required to counter the sophisticated tactics of determined and well-funded foreign adversaries.

Organizations must update their mindset to meet today's threat environment. Now is the time for a high-level, goal-driven assessment of how the U.S. government can better protect national security technologies from foreign theft. While American leadership in AI, biogenetics, and quantum computing remains intact, small businesses and universities urgently need support to protect their hard-won technological advancements.

BACKGROUND

Nation-state threat actors continue to evolve their strategies and tactics for intellectual property theft. The National Counterintelligence and Security Center (NCSC) has warned that both lone threat actors and nation states are "increasingly targeting private sector organizations, state and local governments, and academic institutions".[4] A 2023 *Washington Post* article identified over 300 instances in which U.S. companies sold products to People's Republic of China (PRC)-controlled commercial entities that openly advertised support for the Chinese military.[5]

The CCP prioritizes the theft of national security-related technological data. Under its *Made in China 2025* national industrial plan, the CCP targeted ten critical technologies, including electric vehicles, next-generation telecommunications, advanced robotics and AI, agricultural technologies, aerospace engineering, new synthetic materials, electrical equipment, biotechnology, high-speed rail, and maritime engineering.[6]

The CCP employs a "whole of society" approach to espionage against the United States, leveraging its government agencies, financial institutions, academia, state-owned enterprises, and commercial companies.[7] U.S. laws and federal agencies are poorly equipped to defend against this aggressive strategy, leaving state and local governments, citizens, businesses, and academic institutions vulnerable to CCP incursions.

According to the NCSC report, *Insider Threat Mitigation for U.S. Critical Infrastructure Guidelines,* foreign actors are collecting unprecedented volumes of public and private data. By combining this information with advanced data analytics, they can identify, target, and exploit vulnerable individuals to advance their geopolitical interests at America's expense.[8]

This advanced data analysis leads to highly refined targeting. As reported by the *Wall Street Journal,* "Ordinary civilians are recruited via social media such as Telegram, as well as through the chat functions of popular online games."[9] These individuals are often unaware they are interacting with foreign intelligence operatives.

Beyond human recruitment, the CCP has institutionalized knowledge transfer through programs like the Seven Sons of National Defense, linking universities with military institutions under the military-civil fusion strategy. A review of 865 cases involving CCP espionage, economic espionage, and illegal technology exports revealed that Chinese universities or professors were involved in over 60 cases of espionage. Academic advancement often motivates such research theft, with the Chinese government and universities encouraging these activities.[10] Most cases of research theft from U.S. universities are motivated by opportunities for professional gain within China's academic system.

Economic coercion is another tool frequently used by the CCP against foreign companies operating in China. Western governments often struggle to shield their companies from the pressure to relinquish valuable intellectual property. China's national security laws grant the CCP broad access to data and operations of foreign companies, forcing American firms to train Chinese counterparts, transfer IP, and lobby U.S. policymakers in favor of Chinese interests.[11]

The U.S. legal and governance framework is outdated when it comes to preventing foreign subversion and large-scale intellectual property theft in the digital era. For example, the Foreign Agents Registration Act (FARA) enacted in 1938 to counter Nazi propaganda,[12] was designed for a world of print media, not one dominated by digital communication and social media.

Although legislation exists to curb foreign theft of national security technologies outside the cleared space, enforcement remains fragmented and inconsistent, with no central agency responsible for oversight.

> **Although legislation exists to curb foreign theft of national security technologies outside the cleared space, enforcement remains fragmented and inconsistent, with no central agency responsible for oversight.**

Key regulatory efforts include:

- **The Protecting American Innovation and Development Act of 2024 (PAID Act of 2024),** which added language to the Export Control Reform Act of 2018 to better identify foreign entities misusing emerging technologies.[13]
- **The Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs**, which fund small businesses developing emerging technologies through America's Seed Fund, sponsored by the Small Business Administration.
- **The Bureau of Industry and Security,** which plays a critical role in designating technologies vital to national security.

The Defense Counterintelligence and Security Agency (DCSA) has begun phased implementation of Continuous Vetting (CV) services for the Non-sensitive Public Trust population.[14] Initiatives such as these are steps in the right direction, but far more comprehensive efforts are needed to fully safeguard America's technological edge.

CONCERNS

There is a coordinated, well-resourced campaign by foreign adversaries to exploit vulnerabilities in America's intellectual property protections, particularly within companies and academic institutions operating outside the cleared space. An evidence-based assessment of losses involving critical national security and dual use technologies' reveals several key gaps: lack of awareness, lack of unified and empowered leadership, and lack of resources.

LACK OF AWARENESS

U.S. government agencies and the Defense Industrial Base (DIB) are keenly aware of insider threats and nation-state efforts to steal sensitive information. This awareness is heightened among organizations employing 'cleared' personnel enrolled in CV by the Department of Defense, Department of Homeland Security and other interagency organizations. These threats are further compounded by the departure of cleared personnel, whether through resignation or workforce reductions, stemming from ongoing government downsizing across both federal agencies and industry. To address this known and growing threat, these organizations actively use cyber, physical, and human risk management tools, along with established procedures, investigative practices, and mitigating strategies.

In contrast, awareness is significantly lower within academia and small businesses, especially those at the forefront of technological innovation. These organizations may be developing dual-use technologies with significant national security implications, but operate outside classified environments and lack the tools, knowledge, or funding to adequately protect their work. This is particularly true for dual-use technologies, where innovations intended for commercial or academic purposes may also hold national security applications.

As a result, critical national security technologies often remain unrecognized and unprotected by existing regulations. Awareness typically arises only after high-profile incidents, such as the conviction of former Harvard professor Charles Lieber, which brought national attention to the risks of foreign influence and intellectual property theft in academic settings.[15]

LACK OF RESOURCES

Large firms often have dedicated staff and resources to establish robust insider threat and IP protection programs. However, smaller businesses and academic institutions often lack the funding and infrastructure necessary to implement effective security measures. Some Insider Threat programs require organizations to enroll their employees, contractors, educators, and foreign nationals into federal processes before granting them access to the project. At a minimum, organizations are encouraged to conduct their own background checks, in addition to any vetting performed by external agencies such as the State Department. However, these measures may be prohibitively expensive for smaller entities.

Existing programs intended to support a trusted workforce often lack consistent funding and robust enforcement mechanisms. Additional regulatory burdens, such as those imposed by Federal Acquisition Regulation (FAR) Clause 52.204-21, "Basic Safeguarding of Contractor Information Systems," create further strain. These requirements can be particularly challenging for small businesses in the DIB. A 2024 report by the Commission on the National Defense Strategy found that increased regulatory requirements, combined with economic pressures, have led to a 40% reduction in small businesses operating within the DIB over a 10-year period.[16]

LACK OF UNIFIED & EMPOWERED LEADERSHIP

Although multiple agencies have implemented policies aimed at countering foreign influence within U.S. industries, there is no clear chain of command or single authority for addressing insider theft of national security technologies.

For example, while the U.S. State Department conducts initial vetting of foreign visitors before approving visas, responsibility for ongoing vetting becomes the responsibility of the hosting organization. Agency efforts often operate in silos, with limited coordination or information sharing. This fragmented approach creates exploitable gaps.

Currently, there is no single lead agency tasked with determining which critical technologies require protection, while also balancing the academic need for collaboration and publication. Furthermore, when a visa is issued to a foreign researcher who is later removed from a program or denied participation, there is no automated mechanism to track that change. Universities and the affected foreign researchers are responsible for notifying the State Department of the change in status. Select visa holders (F-1, M-1, and J-1) are required to inform offices within the State Department and Department of Homeland Security, but this information is not automatically shared across systems.

RECOMMENDATIONS

The time is right for a fresh look at how to curb insider theft of American national security technologies. The risks of foreign dominance in revolutionary fields like AI and quantum computing are increasingly clear, and competition with nation-states over these dual-use technologies is intensifying every day.

- **Establish a multi-agency task force** that includes representation from academia, research institutions, and commercial business. This task force should report to the National Security Council within 120 days of its formal establishment via memorandum and be charged with recommending strategies to counter insider theft of national security technologies in the uncleared space. The task force should include senior members of the U.S. Government, Intelligence Community, private sector small businesses to include startups new to the DIB, and academia.

The task force's responsibilities should include evaluating the need to assign a single lead agency empowered to:

- engage directly with companies and universities developing sensitive technologies
- improve enforcement of relevant existing laws
- develop overarching guidance, requirements, and penalties for failures to protect intellectual property within academic and corporate entities.
- provide funding to small businesses and universities for insider threat protection

Additionally, the task force should assess how to better coordinate efforts across agencies and ensure that businesses and institutions receive the support needed to mitigate and combat insider theft of national security technologies.

Specifically, this task force could examine the following countermeasures:

- **Designate a lead U.S. government entity** to develop and implement a unified program of countermeasures against insider theft of national security technologies, with a focus on small businesses and academia. The FBI, given its counterintelligence mission, may be well suited to lead.
- **Identify emerging technologies** likely to attract high interest from foreign adversaries and launch an awareness campaign directed at small businesses and universities developing these technologies.
- **Develop policies and processes like those for cleared individuals.** Publish a NISPOM-like document for uncleared organizations, including an inspection checklist and best practices for protecting sensitive technologies.
- **Clarify through legislation** the criteria for determining which dual-use and emerging technologies warrant protections under national security laws.
- **Require Safeguards for Academic and Corporate Research.** Define, inspect, and enforce policies requiring significant safeguards in bilateral and multilateral research activities conducted by corporate and academic institutions.
- **Establish legal consequences** for individuals identified as engaging in intellectual property or research theft, including prosecution, having their visa revoked, and future visa denials to visit or work in the United States or allied countries.
- **Increase collaboration with allies** to combat insider theft, including the creation of joint exclusion lists to limit access to markets by those engaged in IP theft.
- **Determine the need for new policies** to limit adversaries from acquiring these solutions through stronger due diligence processes when selling dual-use technologies in foreign markets.
- **Prohibit U.S. universities** from conducting research, either jointly or otherwise, with foreign universities or companies on the Department of Commerce Entities List. Violations could result in significant fines or criminal charges.
- **Replace self-certification requirements** for Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs with third-party certification, along with expanded funding to support compliance.
- **Create a funding stream** to help universities and small businesses implement the new requirements that evolve from these recommendations.

CONCLUSION

Much of the development of critical national security technologies occurs within private firms and universities operating outside of the 'cleared space.' To preserve the nation's competitive edge, the U.S. government must do more to protect sensitive technologies from insider theft.

By strengthening protections and offering needed support, the United States can secure its innovation ecosystem, prevent adversaries from exploiting emerging technologies, and maintain its leadership in critical fields like AI and quantum computing.

In the long term, adopting these measures will provide a more secure foundation for collaboration between government, industry, and academia. By acting now, the United States can remain at the forefront of technological innovation while protecting its economic and national security interests against increasingly sophisticated threats.

REFERENCES

[1] *The Stanford Review Staff, "INVESTIGATION: Uncovering Chinese Academic Espionage at Stanford." Stanford Review, May 7, 2025. https://stanfordreview.org/investigation-uncovering-chinese-academic-espionage-at-stanford/.*

[2] *Evanina, William R. "Statement of William R. Evanina CEO, The Evanina Group, Before The House Homeland Security Committee at a Hearing Regarding "Countering Threats Posed by the Chinese Communist Party to the U.S. National Security", Congress, March 5, 2025. https://www.congress.gov/119/meeting/house/117903/witnesses/HHRG-119-HM00-Bio-EvaninaW-20250305.pdf.*

[3] *INSA's Insider Threat Subcommittee. "Insider Threats and Commercial Espionage: Economic and National Security Impacts." INSA. Accessed April 22, 2025. https://www.insaonline.org/docs/default-source/default-document-library/2022-white-papers/insa-wp-espionage-fin-1.pdf?sfvrsn=132d0a1b_4.*

[4] *Seldon, Matt. "NCSC Report Warns of Escalating Insider Threats to Critical Infrastructure HS Today." HSToday, February 28, 2025. https://www.hstoday.us/subject-matter-areas/infrastructure-security/ncsc-report-warns-of-escalating-insider-threats-to-u-s-critical-infrastructure-amid-rising-foreign-espionage-risks/#:~:text=With%20foreign%20adversaries%20and%20cybercriminals,alongside%20cyber%20and%20physical%20threats.*

[5] *Schogol, Jeff. "How Much of a Threat Are Chinese Hypersonic Missiles to US Navy Ships and Sailors?" Washington Post, October 17, 2022. https://www.washingtonpost.com/national-security/2022/10/17/china-hypersonic-missiles-american-technology/.*

[6] *McBride, James, and Andrew Chatzky. "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations, May 13, 2019. https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.*

[7] *"Exposing CCP Espionage." Indo-Pacific Defense FORUM, February 28, 2024. https://ipdefenseforum.com/2024/02/exposing-ccp-espionage/.*

[8] *"Insider Threat Mitigation for U.S. Critical Infrastructure Entities." National Counterintelligence and Security Center. Accessed April 23, 2025. https://www.dni.gov/files/NCSC/documents/nittf/20240926_Insider-Threat-Mitigation-for-US-Critical-Infrastructure.pdf.*

[9] *Pancevski, Bojan. "Europe Sees Signs of Russian Sabotage but Hesitates to Blame Kremlin." Wall Street Journal, May 20, 2024. https://wwwwsj.com/world/europe/europe-sees-signs-of-russian-sabotage-but-hesitates-to-blame-kremlin-72598d4b.*

[10] *Eftimiades, Nick. China's Espionage Recruitment Motivations: Getting Rid of the MICE. European Intelligence Academy. December 2023. https://www.rieas.gr/images/editorial/EIAPaper5.pdf*

[11] *Chafetz, Glenn. "How China's Political System Discourages Innovation and Encourages IP Theft." The SAIS Review of International Affairs , July 31, 2023. https://saisreview.sais.jhu.edu/how-chinas-political-system-discourages-innovation-and-encourages-ip-theft/.*

[12] *Foreign Agents Registration Act (FARA): Background and Issues for Congress, June 30, 2020. https://crsreports.congress.gov/product/details?prodcode=R46435.*

[13] *"H.R.8924 - PAID Act of 2024." Congress, July 11, 2024. https://www.congress.gov/bill/118th-congress/house-bill/8924/text.*

[14] *"Continuous Vetting Enrollment Begins for Non-Sensitive Public Trust Federal Workforce." Defense Counterintelligence and Security Agency, August 12, 2024. https://www.dcsa.mil/About-Us/News/Article/Article/3871107/continuous-vetting-enrollment-begins-for-non-sensitive-public-trust-federal-wor/.*

[15] *"Former Harvard University Professor Sentenced for Lying about His Affiliation with Wuhan University of Technology; China's Thousand Talents Program; and Filing False Tax Returns." United States Attorney's Office District of Massachusetts, April 26, 2023. https://www.justice.gov/usao-ma/pr/former-harvard-university-professor-sentenced-lying-about-his-affiliation-wuhan.*

[16] *US Congress. Commission on National Defense Strategy, Commission Report, page 52. (July 2024). https://www.armed-services.senate.gov/imo/media/doc/nds_commission_final_report.pdf*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Michael Crouse,
Insider Threat Subcommittee Chair, Everfox

Clay Drye, *Everfox*

Michael Hudson, *ClearForce*

Val LeTellier, *4th Gen Solutions*

Nick Eftimiades, *Shinobi Enterprises*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Bishop Garrison, *Vice President for Policy*

Peggy O'Connor,
Director of Communications and Policy

Najim Murshidi, *INSA Policy Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 175+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

INSIDER THREAT SUBCOMMITTEE

ABOUT INSA'S INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Building a Stronger Intelligence Community