Testimony before the Senate Committee on Energy and Natural Resources on "Examining Research Security Risks Posed by Foreign Nationals from Countries of Risk Working at the DOE's National Laboratories and Necessary Mitigation Steps"

Anna B. Puglisi
Visiting Fellow, Stanford University's Hoover Institution
20 February 2025

Chairman Lee, Ranking Member Heinrich, distinguished members of the Committee and staff, thank you for the opportunity to participate in today's hearing and address the committee on this very important topic. It is an honor to be here alongside the esteemed experts on this panel. I am currently a Visiting Fellow at Stanford University's Hoover Institution where I research S&T policy development, global technology competition and research security mitigation strategies. I previously served as the National Counterintelligence Officer for East Asia and for most of my career I have studied China's science and technology (S&T) development and innovation ecosystem, including its efforts to acquire technology and technological know-how.

My testimony today will address why the DOE labs are targeted by China and then discuss research security and potential mitigation strategies. I will discuss how our systems differ, how China's institutions are tools of the state, and how the role of the state impacts and influences all aspects of China's S&T ecosystem including universities, state key labs and commercial entities. Lastly, I'll offer lessons learned, which include:

- This is not just a DOE problem but a U.S. problem. China's system is not the same as our own and it impacts our ability to protect our technology and innovation base. China takes a holistic approach to developing technology—blurring the lines between public, private, civilian and military.
    - Our current mitigation tools are not designed to counter an entirely different system.
- China's government has explicit efforts to exploit its diaspora—and as a result our innovation base. This must be addressed and countered.[i] At the same time, the rights of persons of Chinese ethnicity in the US must be protected despite this deliberate exploitation.
    - Beijing in many ways understands our societal tensions. China's statecraft is directed at them, exploiting identity politics by promoting any changes in U.S. policy as ethnic profiling. It offers a narrative that it is merely a proponent of "development" and science, as a way to divert attention from its own questionable behavior. This is a well-funded effort.[ii]
- We can't protect what we don't have.
    - Scientists–and innovation–will thrive with funding, lab space and freedom to answer hard questions. This is what makes the DOE labs such a tremendous

resource. Sustained funding over time for people and facilities are a key component of technology competition. The investments we make or don't make today will impact our ability to lead and compete tomorrow.

Threats to the DOE Complex: Competition and The Importance of S&T

The U.S. science and technology research enterprise—and especially the Department of Energy (DOE), sets the standard for discovery and innovation excellence globally. DOE is key to U.S. technology competition and in my opinion an underappreciated resource. Through its labs and plants, the DOE builds a technically capable workforce that supports future discovery and industry. More importantly though, DOE's work is also a window into the priorities of the U.S. government.

Historically, collaborations and sharing of data, research and human capital across national borders has always been a U.S. strength. However, it also creates vulnerabilities in our innovation base and the DOE labs as some countries use these collaborations and exchanges to acquire know-how and talent through legal, illegal and extralegal means.

The world has changed since many of the mitigation tools in the toolbox—export controls, CFIUS, FARA and the discussions around how to treat basic research put forth in NSDD-189 were put in place[1]. More pointedly, what we have done in the past regarding research security is no longer working. While I still believe we must embrace open science, our assumption should not be that all collaboration is good until proven otherwise. Unfortunately, some governments have put in place policies and programs to exploit their diaspora and seek collaborations to meet their strategic goals.

Creating a climate to safeguard science will take a mindset change. Our current tools are tactical and narrow by design because they are crafted to mitigate behaviors with the assumption that the actor fully participates in a laws based, rules based system and more importantly plays by the same rules. We know this is not the case for China.

We must recognize that are we in a competition for talent and ideas. We also need to acknowledge that many in the research community see changes in research security as punitive. Even though the policy community has been discussing these issues for almost a decade and has put in motion a lot of new research security requirements, many in the research community still debate whether there is a problem and argue that many of the policies are xenophobic. Because of this it is important to introduce a discussion of benefits and push our research community to do so as well. The "benefit" of collaborations is not always the same across the different stakeholders. We must break it down into the following:

- Does the individual researcher benefit?
- Does the university, lab, business benefit?

[1] NSDD-189, published in 1985 makes the distinction between basic and classified research and is referenced in many discussions regarding research security (https://catalog.archives.gov/id/6879779). FARA is the foreign agents registration act. CFIUS is committee on foreign investment in the U.S.

- Does the U.S. government and taxpayer receive the benefit of the collaboration and investment?

Benefits can be topic and stakeholder specific. An individual researcher can benefit from a specific collaboration because it brings them additional resources, prestige, lower cost labor in their labs and access to data or research equipment. However, that collaboration may not benefit the institution they belong to or the government agency that funds the work because of the loss of data, ideas and potentially intellectual property. There are also potential long-term implications of that loss. Continued dialog is essential to bridge these gaps in understanding.

Countering China's actions will take a team effort. When I meet with researchers, I remind them that there is no free lunch. That is true here today as well if we want to compete with China.

- Researchers need support to find the next cure, new materials or build new military capability
- Agencies need resources to properly vet and protect investments
- There must be a cost on entities or individuals that exploit open collaboration.

Why the focus on China:

China's policies[2] to target the Department of Energy complex are the expression of a deliberate, state-sponsored strategy to save time and money, and "leap-frog" to the international forefront by leveraging the advances of other nations. While military and intelligence related technology are still targeted, China's efforts increasingly focus on technologies of the future such as AI, biotechnology, advanced manufacturing and materials, often in the early stages of development. [iii]

China has demonstrated a willingness to flaunt global norms to reach its strategic goals and has put in place policies and programs that undermine the assumptions built into our system. These include: a fair and level playing field, transparency, reciprocity and market-driven competition.[iv] These actions have far-reaching implications for the future of our nation and our ability to compete. These challenges are not about the concerns of one administration or the policies of one political party, but the actions of a nation-state with a different system, different regard for human rights and different view of competition.

While China is not the only country that targets U.S. technology and the DOE complex, according to the 2023 Annual Threat Assessment[3] "China is the top threat to U.S. technological competitiveness, as it targets key sectors and proprietary commercial and military technology from the U.S. and allied companies and institutions." This puts the DOE complex directly in the crosshairs given the depth and breadth of its mission. What is clear is the following:

- China has a whole of nation approach to acquiring technology and knowhow

[2] Please see These policies include "two bases formula", "short-term visits" and "serve in place. See Hannas et al., Routledge 2013 more a more in-depth treatment of these policies.
[3] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

from around the world.

- China views technology as a national asset.
- China has stated that it wants to dominate in the industries of the future—AI, biotechnology, advanced manufacturing and materials. All areas the DOE labs are focused on.
- All parts of Chinese society – academia, private sector, government –and all aspects of the research ecosystem --technology R&D, economic development, military modernization are controlled by the Chinese Communist Party at varying levels.
- China targets unclassified R&D before it is placed into protected areas (e.g. export controls or classified programs).
- China pursues knowhow, processes, and methodologies that it can then apply to weaponize and commercialize technology at US expense.
- China sees its diaspora as a conduit for technology and technological knowhow.

Today's hearing is about the risk to the DOE labs posed by individuals from countries of concern. It is well documented[v] that foreign talent is key to China's technology acquisition strategy. China uses non-traditional collectors—expert scientists, businesspeople and students--to acquire technology and technological knowhow. Our system—and I would add our institutions and the authorities we have granted them—is not designed to counter this kind of threat. Traditionally counterintelligence has focused on intelligence officers, military end-use and illegal activities. I tell you today, if we only focus on trying to mitigate China's illegal actions, those undertaken by intelligence officers or are related to military technology, we will fail. These non-traditional collectors are rarely in CI databases—they are not intelligence officers. Our current mitigation system is not designed to identify and counter them. The protections in the CHIPS act and NSPM-33, and as a result the individual programs put in place at agencies such as DOE and NSF are a good start, but it will take a comprehensive centralized effort to fully counter China's actions.

Moving forward we must be honest with ourselves, our researchers and the world. While there are a lot of discussions about "de-risking," sometimes you can't "get to yes" because of the sensitivity of topics or the affiliations of the institutions and people involved. This is because of the choices of a nation state that seeks to exploit our system and openness, not because of U.S. policy or actions. The U.S. and international science and engineering enterprise is put at risk when other governments seek to benefit from the global research system without upholding the tenets of research integrity and sharing equally.

There are actions we can take to better protect our investments, not only at DOE but across the U.S. research enterprise. Reviewing both access to the labs and funding decisions should address the following issues:

- Does the entity have foreign ownership or control?
- Are there criminal or regulatory issues related to the entity or individual?
- Will this collaboration or development create dependencies in supply chains?
- Will the individual have access to sensitive equipment, supplies or data?
- Does the individual have ties to malign foreign talent recruitment programs or other kinds of conflict of commitment?

- What kind of foreign funding sources are involved (both monetary and in-kind)?
- Are there concerning behaviors or obfuscation associated with patenting to include transferring information to foreign entities after filing, filing in a foreign country without the DOE collaborators etc.
- Are there ties to foreign entities or foreign collaborators on specified lists or with specified characteristics?

However, while reviewing these individual factors are important, a more comprehensive mitigation strategy is needed. I put forth the following elements as part of a national level program. Piecemeal solutions that are not at scale will not have the desired outcomes. While different agencies with different missions won't have the same risk threshold, all should start with the same level of information and make data-driven decisions.

Establish a National Center for open-source information. This national level resource would provide background information and help researchers, universities and national labs make informed decisions. This information center (center) should be part of the US government or an FFRDC, and interact with the IC, but not be a part of the IC. This center would be the connective tissue that enables a fuller understanding of technology developments and development networks, centers of excellence globally, and connections to malign actors. While there have been past and current efforts to do this, they are not sufficient and are not at scale.

"Precheck" For Collaboration: The U.S. and likeminded countries must create clear standards, norms, and expectations for visiting researchers, post-doctoral scientists and students. Working with our allies and like-minded countries is essential to protecting our respective innovation bases. Developing an international agreement—including verification mechanisms—will enable collaborations while guarding against the actions of nations that do not adhere to global norms. An accepted framework of protections will enable streamlined risk-management processes for collaborations among member countries, their institutions, and principal investigators—a kind of PreCheck lane for approval.[4]

Invest in the Future: Infrastructure and STEM talent. The United States and other liberal democracies must invest in their futures. Not all jobs of the future will require a university degree, but they will require more specialized training. We also must remember that innovation comes from doing the research—if we are not doing the research, we will not be innovative. Growing domestic talent and technical infrastructure so our scientists do not have to go to our strategic competitors to do their research will be essential. The investments we make or do not make will impact our future competitiveness and ability to grow our economy and sustain our military capabilities.

[4] For a more comprehensive discussion of this proposal please see: https://www.hoover.org/research/how-create-and-sustain-rd-leadership

Figure 1: Above is a graphic representation of China's S&T development and technology transfer efforts. China takes a holistic approach to developing its S&T infrastructure and employs all facets of its government and society to acquire technology.

CONCLUSIONS:

China takes a holistic approach to development, blurring what is civilian, what is military, what is private and what is public. This has deep implications for the DOE complex because it impacts the basis for entry of Chinese students and post-docs into U.S. labs. China's laws which include the ability to compel citizens to share information also complicates the ability for individual researchers to act independently. Existing export and visa policies that build their restrictions around affiliations with a military end-user but make exceptions for civilian uses have limited affect. To the Chinese leadership, every civilian use is also a potential military use.

In moving forward, I leave the committee with the following thoughts:

- We must decide what winning looks like—this will take a comprehensive strategy.

- Extreme propositions, such as closing our eyes (laissez faire) or closing our doors, only benefit China. We either discredit all efforts to address the problem or deprive ourselves of the contributions of foreign-born scientists.

- China is not a neutral actor. Why does this matter? China intimidates and harshly silences its critics. This has only grown in the past few years and places individuals in untenable situations. We do our foreign students and colleagues a disservice by not highlighting China's actions.[vi]

In closing, I want to thank the committee again for continuing to discuss this issue. These are hard conversations that we as a nation must have if we are to protect and promote U.S. competitiveness and future developments. These conversations will make us uncomfortable because they challenge assumptions and established norms. If we do not highlight and address China's policies we give credence to a system that undermines fairness, openness and human rights. Thank you.

---

[i] E.g., "The IP Commission Report." The Commission on the Theft of American Intellectual Property (May 2013). Hannas, Mulvenon and Puglisi, *Chinese Industrial Espionage*. (Routledge, 2013) hereafter "*CIE*." Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy" (DIUX, February 2017). Section 301 *Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*. Office of the United States Trade Representative (27 March 2018). US-China Economic and Security Review Commission, "2019 Annual Report to Congress" (November 2019).

[ii] William C. Hannas and Didi Kirsten Tatlow, *Beyond Espionage: China's Quest for Foreign Technology* (Routledge 1st edition, September 2020); Alex Joske, "Hunting the Phoenix," Australian Strategic Policy Institute, 2020, https://www.aspi.org.au/report/hunting-phoenix ; Receipts of local UFWD paying overseas scientists available at: "The distribution list of provincial-level projects for the introduction of foreign intelligence special funds at the provincial level in 2018" [2018 年省级引进国外智利专项经费直项目分配明细表], https://web.archive.org/web/20201112190122/http://webcache.googleusercontent.com/search?q=cache%3AKAaZ3LpEe4oJ%3Arst.hunan.gov.cn%2Frst%2Fxxgk%2Ftzgg%2F201802%2F9516964%2Ffiles%2Fe1c7ddd51dda49f6b70a6ad5ae9b0490.xls+&cd=3&hl=en&ct=clnk&gl=us

[iii] Hannas, Mulvenon and Puglisi, *Chinese Industrial Espionage*. (Routledge, 2013) hereafter "*CIE*." E.g., "The IP Commission Report." The Commission on the Theft of American Intellectual Property (May 2013). Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy" (DIUX, February 2017). Section 301 *Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*. Office of the United States Trade Representative (27 March 2018). U.S.-China Economic and Security Review Commission, "2019 Annual Report to Congress" (November 2019).

[iv] E.g., "The IP Commission Report." The Commission on the Theft of American Intellectual Property (May 2013). Hannas, Mulvenon and Puglisi, *Chinese Industrial Espionage*. (Routledge, 2013) hereafter "*CIE*." Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy" (DIUX, February 2017). Section 301 *Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*. Office of the United States Trade Representative (27 March 2018). U.S.-China Economic and Security Review Commission, "2019 Annual Report to Congress" (November 2019).

[v] These policies include “two bases formula”, “short-term visits” and “serve in place. See Hannas et al., Routledge 2013 more a more in depth treatment of these policies.

[vi] Roth, Kenneth “China’s Global Threat to Human Rights”, Global Report 2020