

RPTR KERR

EDTR HOFSTAD

CHINA'S ECONOMIC ESPIONAGE AND SUBNATIONAL
INFLUENCE IN THE UNITED STATES

Thursday, June 25, 2026

House of Representatives,

Select Committee on the Strategic Competition Between
the United States and the Chinese Communist Party,
Washington, D.C.

The committee met, pursuant to call, at 10:33 a.m., in Room 390, Cannon House Office Building, Hon. John Moolenaar [chairman of the committee] presiding.

Chairman Moolenaar. The select committee will come to order.

And good morning, everyone. Thank you for being here.

And, before we begin, I want to acknowledge a new member of the committee, our good friend from New York, Representative Tom Suozzi.

Welcome. It is great to have you on the committee.

Today's hearing is on the Chinese Communist Party's economic espionage and malign influence targeted at the subnational level. This is an active threat, and we will examine how these activities have accelerated in scale, intensity, and sophistication over the past decade.

The CCP's professed desire for constructive relations, its pursuit of so-called win-win outcomes, and its supposed respect for the sovereignty of other nations are all promises the CCP breaks.

The CCP is engaged in an epic campaign to undermine the United States here at home, spanning economic and traditional espionage, state-directed cyber intrusions, talent recruitment programs, information warfare, covert influence networks, legal and illegal lobbying, blackmail, infiltrating our critical infrastructure, and transnational repression aimed at the Chinese diaspora.

In fact, the CCP is the largest oppressor of Chinese people in the world, and it has targeted Chinese-Americans who courageously speak out against it.

Just last month, Eileen Wang, the mayor of Arcadia, California, which is home to 60,000 people, was arrested for acting as an illegal agent of the Chinese Government for activities undertaken before she was mayor. She pled guilty and is now in prison.

This Chinese Government agent, acting at the direction of PRC Government officials, took advantage of our free and open society to carry out an agenda on behalf of the CCP. This is an alarm bell for all of us that the CCP's malign influence must be confronted.

United Front Work, one of the CCP's primary instruments for political influence, is a core

component of this strategy. What makes it uniquely concerning is that it is not simply a foreign intelligence activity conducted from afar; it is a comprehensive influence operation that reaches deep into communities, businesses, and institutions across the United States, offering seemingly benign cultural, academic, or commercial engagement.

It operates by exploiting these three primary levers: access, coercion, and incentives.

First, it seeks to access State and local officials, business leaders, university researchers, and community organizations. In many cases, this access is earned through partnerships that appear mutually beneficial -- trade delegations, sister city relationships, student exchanges, or local investment initiatives. However, these channels can be repurposed to collect strategic information, shape local decision-making, or identify individuals who can be influenced or co-opted.

Second, coercion plays a central role. The CCP cruelly exploits vulnerabilities among diaspora communities, including family ties in China, business dependencies, or immigration concerns. Individuals may be pressured, subtly or directly, to support party-aligned positions, silence criticism, or pass along information. These coercive tactics are often deliberately obscured, making them difficult for local authorities or community organizations to detect, let alone counter.

Third, the CCP employs a wide spectrum of incentives. These include commercial benefits, political access, or opportunities for personal advancement. Yet these promises often come with expectations -- that local officials will support PRC-backed initiatives, that academic partners will share research, or that community leaders will echo narratives favorable to Beijing.

The CCP does not distinguish between national and subnational targets. State legislatures, municipal governments, school boards, public universities, local businesses, and community associations are all soft targets. A strategic investment pitch to a mayor, a partnership with a local university, or outreach to diaspora civic groups can yield long-term advantages for the CCP's objectives.

Because these engagements often occur far from Washington, they can unfold with limited

oversight, inconsistent safeguards, and uneven awareness of the risks involved.

This gap between Federal insight and local exposure represents one of our most significant vulnerabilities. Closing it requires sustained collaboration across all levels of government.

Federal agencies must share actionable intelligence and best practices with State and local partners in ways that are clear, accessible, and timely. Local leaders, from mayors to university administrators to community officials, must be equipped with guidance that helps them distinguish legitimate engagement from attempts at manipulation or exploitation.

Above all, our response must reflect the same whole-of-society approach that the CCP employs. Protecting our economic competitiveness, safeguarding our research, and strengthening the resilience of our communities requires participation from government, industry, academia, civil society, and diaspora communities.

The goal is to have an honest and open cultural and economic exchange that is transparent, secure, and mutually beneficial.

Today's hearing will highlight the CCP's continuing abuse of the United States' sovereignty and the divergence between the CCP's words and their deeds. The hearing will focus on two fronts of this battle that demand action from Washington: the CCP's economic espionage and its malign influence at the state level.

More importantly, we hope that today's hearing will provide an important step toward building that coordinated, nationwide response.

Thank you.

And I now recognize the ranking member for his remarks.

[The statement of Chairman Moolenaar follows:]

***** COMMITTEE INSERT *****

Mr. Khanna. Thank you, Mr. Chairman. And I appreciate the bipartisan way you have conducted this committee and your leadership.

I share the concerns about China's economic espionage. It is undisputed that they have stolen intellectual property from American manufacturers, that they require coercive joint-venture agreements. Our companies went there and, basically, to have access to the market, were required to give up intellectual property. And they have tried to get intellectual property from our technology companies and our manufacturers, and we need to stop that.

We need to stop the offshoring of our jobs to China, the offshoring of our industrial base to China, and, certainly, make sure that we have a level, fair playing field. We don't steal China's technology; they shouldn't be stealing ours. We don't have economic espionage with China; they shouldn't be having economic espionage with us. And we need to have self-reliance on critical industries in this country.

And so I look forward, on that, to working on a bipartisan basis.

But I do want to also, as an Asian-American, as a son of immigrants, speak to the United States' troubled history with discrimination based on race or national origin. And I appreciate Mr. John Yang being here to help provide that perspective, which is so important as we consider the real threats that the United States faces.

You can go back to Frederick Douglass and his "Composite Nation" speech in 1869 where he stood up for the rights of Chinese immigrants. And soon after Douglass's urging that we have Chinese immigrants in the United States, unfortunately the country went in a different direction. They had the 1882 Exclusion Act.

We have had a history of discriminating against Asian immigrants to be citizens, to own land. And we had this awful thing called the China Initiative, which Mr. Yang has done incredible work on, which basically went after Chinese-American professors and Chinese-American scientists and made

them feel unwelcome, made them feel profiled, harassed them. And now it has been discontinued because they recognize that Chinese-Americans actually contribute to the United States.

Did you know that, of the top AI researchers in the United States, 38 percent of them are of Chinese origin? We would not have Silicon Valley if we did not have the Chinese-origin top AI researchers in this country. Jensen Huang, who leads the entire AI revolution, is someone who was of Chinese origin. The reality is that the top 72 percent -- of STEM graduates, 72 percent of them come from countries outside of the United States.

So I am very passionate, Mr. Chairman, that, as we look at the legitimate threats that Chinese Government poses to America's economic independence, we do not in any way conflate it with the harassment of Chinese immigrants, of Chinese-Americans, of Chinese students and we recognize the incredible value and role that they play in the United States.

So I look forward to that conversation and hope we can keep that distinction in mind.

[The statement of Mr. Khanna follows:]

***** COMMITTEE INSERT *****

Chairman Moolenaar. Thank you, Ranking Member. And I totally concur with making that distinction. And our goal is really to have policies that protect Chinese-Americans and make sure they have their constitutional rights just like every American should have and free from the CCP's malign influence. So I think we are in total agreement on that.

I also just want to recognize today that we are joined by our friend Representative Jason Smith, who is the chairman of the Ways and Means Committee.

And we are honored to have you here with us today.

And I ask unanimous consent for Chairman Smith to offer a statement.

And, without objection, I recognize Chairman Smith for 5 minutes.

Mr. Smith of Missouri. Thank you, Chairman Moolenaar, Ranking Member Khanna. It is a true honor to be here with you all this morning. Thanks for having me.

I commend you and your fellow committee members for the important work you all have been doing to expose efforts by the Chinese Communist Party to infiltrate and influence our Nation's economic activities as well as our political and public discourses.

I particularly appreciate the working relationship our two committees, the Select Committee on China and the Ways and Means Committee, have had when it comes to combating China's harmful influence.

That includes the letter that Chairman Moolenaar and I led to Treasury Secretary Bessent and IRS CEO Bisignano earlier this year calling on Treasury and the IRS to examine tax-exempt organizations right here in the United States that have close ties to the CCP.

Specifically, we raised concerns about China's United Front tax-exempt organizations that are peddling communist propaganda and influencing our elections in violation of their tax-exempt status.

The Ways and Means Committee has spent years -- years -- investigating tax-exempt organizations. We have found that several of these organizations, which enjoy generous, generous

financial benefits due to their tax-exempt status, have been causing chaos and stoking violence in our communities while also interfering in our political system.

What is even more shocking is the level to which these U.S.-based organizations are funded by foreign nationals that are influenced by foreign governments -- most notably, China.

Our oversight investigation into the Chinese Communist Party's efforts to meddle in our public discourse has uncovered a large network of U.S.-based tax-exempt organizations tied to Neville Roy Singham, a wealthy American tech mogul who operates his network out of Shanghai.

"Shanghai Singham" enjoys close ties to the CCP and shares office space with a Chinese propaganda company which says its goal is to, quote, "tell China's story well." Mr. Singham has also participated in a workshop about promoting the CCP internationally.

During a hearing of the Ways and Means Committee earlier this year, an expert witness testified to how the Singham network mobilizes, trains, and amplifies protests to vandalize property, burn our flag, assault local law enforcement officers, shut down airports and bridges in major cities like New York City and Los Angeles, all in an effort to harm our institutions and disrupt our way of life.

The Ways and Means Committee is seeking information and documentation from the three Singham network organizations -- BreakThrough News, Tricontinental, and the People's Forum. The People's Forum alone received over \$20 million from the Singham network. We have made it clear to all three that we will use every tool at our disposal, including congressional subpoena powers, to conduct our oversight responsibilities.

Most recently, though, Mr. Chairman, foreign money from CCP-aligned sources has flowed into U.S. nonprofits protesting data centers in what we can only assume is an attempt to undermine America's position as the global technology leader.

China would like to dominate the future of artificial intelligence, and it is clear that they are actively seeking to exploit Americans' legitimate -- Americans' legitimate concerns and sow discord in

our own backyard for one purpose, and that is to seize this technological advantage for themselves.

Americans have every right to question the size, the scale, and scope of projects in their backyard, but we cannot, Mr. Chairman, allow the U.S. Tax Code to be weaponized against our national-security interests.

We will follow the money and get to the bottom of the dark web of funding sources and fiscal sponsorships that support rogue tax-exempt organizations, often at the behest of the Chinese Communist Party.

I want to thank you again, to all the members of the China Select Committee, Chairman Moolenaar, Ranking Member Khanna, for continuing to investigate the harmful influence China and its proxies are having on American communities. This work is incredibly important, not only to protect the integrity of our tax laws that govern and provide generous benefits to many of these organizations, but also to the safety and security of our communities and the health of our society.

Thank you once again for having me.

[The statement of Mr. Smith of Missouri follows:]

***** COMMITTEE INSERT *****

Chairman Moolenaar. Thank you, Chairman Smith.

If any other member wishes to submit a statement for the record, without objection, those statements will be added to the record.

I would now like to welcome and introduce our three witnesses today.

Mr. David Shedd served as Acting Director of the Defense Intelligence Agency following a distinguished career in the intelligence community. He is also the author of a new book published this year, "The Great Heist: China's Epic Campaign to Steal America's Secrets."

Mr. Michael Lucci is the founder, CEO, and chairman of State Armor, which is doing important work in equipping State and local governments with the necessary legal tools and policy solutions to deal with global security threats.

Mr. John Yang is the president and executive director of Asian Americans Advancing Justice, which focuses on civil rights for Asian-Americans through advocacy, education, and litigation.

And, with that, I want to welcome all of our witnesses today and thank you for being here this morning.

Mr. Shedd, you are now recognized for your opening remarks.

STATEMENTS OF DAVID SHEDD, FORMER ACTING DIRECTOR OF THE DEFENSE INTELLIGENCE AGENCY; MICHAEL LUCCI, FOUNDER & CEO OF STATE ARMOR; AND JOHN C. YANG, PRESIDENT AND EXECUTIVE DIRECTOR OF ASIAN AMERICANS ADVANCING JUSTICE

STATEMENT OF DAVID SHEDD

Mr. Shedd. Thank you, Mr. Chairman.

Chairman Moolenaar, Ranking Member Khanna, distinguished members of the Select Committee on China, thank you for this opportunity to speak today about one of the most pressing threats in the free world -- China's unprecedented campaign of industrial espionage, that is.

As former Acting Director of the Defense Intelligence Agency who spent decades in the intelligence community and on the National Security Council staff, I want to thank you for the opportunity to speak today about this epic campaign to steal America's industrial secrets.

In 1984, Deng Xiaoping, the successor to Chinese Communist Party Chairman Mao Zedong, reset the strategic direction of the CCP. His vision has been implemented by successive Chinese leaders, including Xi Jinping, since 2012. Deng underscored that China would retain ideological stability -- code words for the CCP's single-party rule -- but would introduce managed capitalism under socialist guardrails to enable social transformation.

China's economic transformation took off in earnest once China joined the World Trade Organization in December 2001, during the period that I was in the White House NSC staff.

Since then, China has orchestrated a highly strategic, highly accelerated, and multifaceted effort to steal commercial and technological secrets from the United States and other Western nations. The campaign, which blends cyber espionage, human intelligence, academic collaboration, and commercial investments, has been instrumental in propelling China's rapid economic and

military rise.

Since joining the WTO, China has transformed from an economic backwater into a global superpower, leveraging stolen technology and property to dominate critical technologies such as telecommunications, artificial intelligence, quantum computing, hypersonic weapons, biotechnology, and, yes, even in the agriculture sector. No commercial area is out of bounds for China's reach.

China's approach is unique and revolutionary. Unlike traditional espionage that I know a little something about, which typically targets government-to-government classified information, Beijing has adopted this whole-of-society strategy.

Under Xi, the security intelligence capabilities of the Ministry of State Security have ballooned in size, vastly outstripping the CIA, the NSA, the DIA, and the FBI. Their mandate is to carry out the world's greatest and grandest larceny.

The CCP's strategy fuses military and civilian collection objectives, and the People's Liberation Army has the first rights to use purloined commercial proprietary intelligence to enable its vast military modernization.

Corporate America, professors, academic researchers are all fair targets for the MSS. The CCP has weaponized venture capital, private equity, and academic partnerships to acquire sensitive technology, research and development, and intellectual property that it could not obtain legally.

This decentralized but highly strategic collection method -- combined with theft, graft, hacking operations -- has allowed China to leapfrog the West in key areas of innovation.

The implications of this campaign are profound. Emerging technologies are the battlegrounds of great-power competition today, and China's theft of secret threats -- the theft of the secrets threatens not only the national security of Western nations but also the competitive standing of their companies in the global marketplace.

As former Attorney General Eric Holder aptly stated, there are only two categories of companies affected by the trade-secret theft from China: those who know that they have been

compromised and those who don't.

Yet many private-sector leaders remain oblivious to the long-term consequences of fueling Chinese economic superiority in pursuit of short-term profits.

Western governance and security apparatuses have failed to react appropriately to safeguard against the CCP's steadily evolving campaign of theft. Traditional legal and regulatory frameworks are ill-suited to address the modern tactics employed by China, making prosecution of trade-theft cases difficult, even when evidence is overwhelming.

As Secretary of State Marco Rubio has warned, American companies are committing corporate suicide -- and I quote -- "by failing to prioritize IP security and guard their assets."

This is not just a commercial war; it is a unilateral campaign by China to reshape and dominate the global order. In "The Great Heist," my co-author, Andrew Badger, and I document this systematic campaign driven by initiatives such as Made in China 2025, which was launched in 2015 and represents, according to former FBI Director Chris Wray, the largest transfer of wealth and knowledge in history, estimated to be about \$600 billion annually.

While direct military confrontation is not inevitable, the risk of a hot war over Taiwan grows with each passing day. CCP Chairman Xi has declared his intent to reunite the island by 2027, and, of course, this could happen even sooner. Such a conflict would likely involve deployment of new lethal technologies and could target the American homeland itself.

I urge policymakers and U.S. corporate leaders to recognize the gravity of these PRC/CCP actions and take decisive actions to protect our national interests and secure the future of the free world.

I welcome your questions and, once again, thank you for the opportunity to be a part of this very important hearing.

I yield back.

[The statement of Mr. Shedd follows:]

***** COMMITTEE INSERT *****

Chairman Moolenaar. Thank you very much.

Mr. Lucci, you may proceed.

STATEMENT OF MICHAEL LUCCI

Mr. Lucci. Chairman Moolenaar, Ranking Member Khanna, and members of the committee, my name is Michael Lucci. I am the founder and CEO of State Armor, a nonprofit that works with State governments to protect the American homeland.

My message is simple: The American homeland is contested. States are on the front lines of this contest. And the Chinese Communist Party is exploiting vulnerabilities at the State and local level that can go overlooked here in Washington, D.C.

My remarks will focus on prepositioning near critical assets, influence operations, their impact on State institutions; State protective responses, with a focus on Nebraska and Texas; and, finally, the pressure campaigns that have been put upon these State lawmakers who have enacted these protective responses.

First, on prepositioning, Federal leaders have been very clear that the Chinese Communist Party is prepositioning on critical infrastructure and creating vulnerabilities in our supply chains. What State leaders find is that they are also physically prepositioning near military installations.

I will give just a few examples.

A former officer in the People's Liberation Army bought 140,000 acres near Laughlin Air Force Base in Texas, where he tried to directly access the Texas energy grid near the base.

Huawei equipment surrounded nuclear missile silos in western Nebraska.

Fufeng Group was building a grain silo 12 miles from Grand Forks Air Force Base until the Air Force itself said that this was a clear national-security threat.

Governor Cox of Utah removed a CCP front company from its industrial location near a weapons testing facility in Utah.

And then property owners tied to Chinese intelligence have been found with properties that literally touch the fence lines of Whiteman Air Force Base and Barksdale Air Force Base in Missouri and in Louisiana.

Such prepositioning allows for surveillance -- someday, it could allow for sabotage -- of those assets. States have taken action to mitigate these threats that they see in their backyard.

On influence operations to penetrate State institutions, from our view, the penetration of universities is a national-security crisis. The interference operations in statehouses, which I will discuss later, is a scandal.

Reports from this committee have documented thousands of federally funded, military-focused grants that go to American universities, who then turn around and partner with entities in China tied to China's military and defense industrial base to develop military technologies.

So the way we see it is, we are funding their military modernization through our Pentagon grants, Department of Energy grants. These partnerships are inexcusable, but, from what we have seen, they are the tip of the iceberg for infiltration of our universities.

In terms of State responses, Nebraska and Texas have been the leading States. Most of this work has been bipartisan.

In Nebraska, in particular, Republican Governor Jim Pillen partners with State Senator Eliot Bostar of Lincoln, a Democrat, for the best model of bipartisan teamwork at the State level.

In Texas, Governor Abbott has led with executive orders, and the legislature has enacted overwhelming bipartisan responses to protect State assets in Texas.

I will give you a few examples of what has occurred in these States: creation of committees to prepare for the fallout, the domestic fallout, of a Pacific conflict; military critical infrastructure and supply chain protections; foreign agent registration for adversary nations; bans on Chinese

Communist Party funds in lobbying in statehouses; the first laws in the country on transnational repression came, first, in Texas and then, second, in Nebraska; protections of research security and campus integrity; pension divestment; and protecting genetic data of Americans from the People's Liberation Army. Finally, Texas even created a State Cyber Command to counteract threats that are hitting small communities across Texas, rural and otherwise.

In addition, the attorneys general of these States, Mike Hilgers in Nebraska and Ken Paxton in Texas, have driven consumer-fraud cases against Chinese technology providers based upon the claim that these technologies contain backdoors or dangerous malware that is not disclosed to the consumer. They have worked with the FCC on this project.

Yet, when States push back against threats, they encounter sophisticated pressure campaigns. Jamestown Foundation's Cheryl Yu describes how the Chinese Communist Party's United Front system co-opts individuals, nonprofits, and businesses to advance party interests. This happens in statehouses.

State Senator Eliot Bostar testified earlier this month before the CECC that he personally received threats from a large Chinese business in the State of Nebraska about what might happen to the economy of Nebraska if Senator Bostar's foreign agent registration bill advanced.

Governor Pillen of Nebraska has come out and said that he would prefer that Chinese Communist Party companies that engage in this behavior just leave the State of Nebraska.

Digital threats have been sent to people who testify in front of committees in Nebraska. Omaha reportedly has a United Front service station.

In Texas, lawmakers and Chinese-Americans who testify in committee in favor of these protective measures have received threats. Chinese Communist Party state media talking points are repeated in hearings for hours in Texas, even when they have no relation to the underlying bill. Pastor Bob Fu in Texas has been a victim of transnational repression.

There was even a hearing of Texas's equivalent committee of your committee -- so Texas had

a committee on foreign-adversary threats. That hearing was shut down by a cyber attack in September of 2024.

This is not normal advocacy. It is a pressure campaign from a non-democratic actor acting within our democratic system. It happens across the country, although I highlight just the examples of Nebraska and Texas today.

Our openness is a strength. So is our federalist system. But our open system cannot endure endless attacks and exploitation from state actors who do not agree with our democratic values.

Thank you for addressing these concerns, thank you for interest in influence operations at the subnational level, and I look forward to your questions.

[The statement of Mr. Lucci follows:]

***** COMMITTEE INSERT *****

Chairman Moolenaar. Thank you.

Now let's turn to Mr. Yang.

STATEMENT OF JOHN C. YANG

Mr. Yang. Thank you very much. Thank you, Chair Moolenaar, Ranking Member Khanna, and members of the select committee.

Good morning. My name is John C. Yang. I am the president and executive director of Asian Americans Advancing Justice, which is a national advocacy organization that advances the civil and human rights of Asian-Americans and seeks to promote a fair and equitable society for all.

This committee was created to confront the security challenges that the Chinese Communist Party presents to the United States. We do not dispute that this challenge is real, just as the challenges imposed by the Putin regime and any other autocracy is real. These governments are autocracies and dictators, and they do not respect civil rights, human rights, or democracy.

That said, my purpose here today is to help this committee address these challenges without repeating the mistakes that our country, unfortunately, has sometimes made in the past, substituting ethnicity-based suspicion for evidence-based enforcement in the name of national security.

When we in the United States have failed to recognize the distinction between governments and the people subjugated and ruled by those governments, we have subjugated people in our country, often our own citizens and residents, to harm and discrimination. Unfortunately, Asian-Americans have too often been the victim in the name of national security.

Now, this risk is not hypothetical. We saw the lynching of Chinese-Americans and the passage of the Chinese Exclusion Act when some believed that Chinese laborers, some of the same laborers that helped to build the transcontinental railroad, were taking jobs from White Americans.

We saw the incarceration of Americans of Japanese descent during World War II and the murder of Sikh Americans and countless hate crimes against Arabs, Muslims, Middle East, and South Asians after 9/11. More recently, we experienced tens of thousands of hate incidents, not to mention physical violence, against the Asian-American community because of COVID-19.

In each of these cases, there were legitimate concerns related to foreign affairs, but in each of these cases, our domestic community, our fellow Americans, were harmed.

Unfortunately, this is not a vestige of a bygone era but, rather, manifests itself in policies today. As many of you know, your colleague, Representative Judy Chu, has been faced with accusations of divided loyalty simply for her stalwart advocacy on behalf of the Chinese-American community. More recently, Maryland Delegate Chao Wu has been slandered, in part simply because he has an accent. These are not the profiles of foreign agents. These are the profiles of Americans serving our country.

Policies and initiatives have likewise unfairly targeted the Chinese-American and broader Asian-American community. The Department of Justice's China Initiative, launched in 2018, shifted from targeting people acting on behalf of the Chinese Government to targeting scientists and researchers who simply had a nexus to China. Most cases involve no espionage charges at all but, rather, involve administrative errors on disclosure forms.

When considering policies meant to combat state-based espionage and subnational influence, I would ask lawmakers to engage in a thorough cost-benefit analysis with the nuance necessary to develop real solutions to precise problems. Saying that a policy will benefit national security is too simplistic and does not lead to effective results.

On the other side of the ledger, the cost to the Asian-American community is clear. Surveys conducted by Pew and The Asian American Foundation found that one in two Asian-Americans no longer feel safe because of their race or ethnicity.

The number of scientists and students that are interested in coming to the United States, not

just from China but from countries all over the world, is dwindling. This brain drain does not benefit national security. National security is not only about keeping bad actors out; it is also about keeping good, innovative contributors in.

I offer this committee five specific recommendations for developing policies that will have a net benefit to America without unnecessary cost.

First, let's predicate policies on specific, articulable evidence of conduct, not ancestry, and ensure that anyone charged with enforcing those policies have the proper training and expertise to determine wrongful conduct.

Second, avoid over-criminalizing administrative errors, and ensure that resources are devoted to investigating issues where security is truly threatened.

Third, tailor ownership or lending restrictions to actual indicators of foreign-government control, not ordinary immigrant family ties.

Fourth, build anti-bias training, civil rights, due-process protections, along with a reporting mechanism that ensures transparency in our system.

And, fifth, invest in language access and education to ensure that our communities receive the information they need to contribute to our economy and our security.

Finally, I urge this committee to pair enforcement with renewed people-to-people exchange. Asian-Americans are not a security liability to be managed. We are an asset, a community uniquely positioned to rebuild the scientific, academic, and business ties that have historically reduced conflict between nations.

A targeted approach is not necessarily a softer approach; rather, it is a more effective one.

Thank you very much. I look forward to your questions.

[The statement of Mr. Yang follows:]

***** COMMITTEE INSERT *****

Chairman Moolenaar. Thank you.

Now we would like to turn to questions, and I will recognize myself for 5 minutes of questions.

Mr. Shedd, you have discussed the importance of protecting the crown jewels of American technology, including our cutting-edge AI models.

This week, news broke that Alibaba targeted Anthropic with a distillation attack to steal Anthropic's intellectual property. Given your expertise in China's espionage methods, what does this tell us about how China is targeting our technology?

Mr. Shedd. Thank you for that question.

You hit on a keyword, "distillation." And perhaps the audience doesn't know the term, but essentially it is simplifying the data that is in very expensive models that have been built by Anthropic and others in terms of artificial intelligence that then the Chinese are taking that data and, if I can use the term, "dumbing it down" in order so that they can put it on the market at a much lower cost and with greater accessibility to it.

So it tells me that we are looking at the CCP's ability to generate new requirements and new capabilities around adopting to the transformation and the growth of AI.

So, when we look backwards and look at DeepSeek, as an example, when they rolled that out, their capabilities surprised many, in terms of having their own version of ChatGPT. And, in doing so, it told me that they are on the path of monetizing but then also accessing the data of all users that would have anything to do with these models, that then they distill from these much larger and expensive models.

But the bottom line is financial as much as it is the intelligence collection as well. They are able to bypass the investment that these large AI companies in the United States have put into it, whether they are still in private equity or outside of that or on the path to becoming an IPO, and,

therefore, don't have to invest in that area and simply leapfrog into having it.

So it tells me that their great heist continues in the area of both data and technology, with regards to what they appear to be doing with Anthropic and the distillation of these models.

Chairman Moolenaar. And following up on a related topic, but if there was one action that Congress could take today to raise the cost of the CCP's malign-influence operations against the United States, what would it be? What would the one thing we could do be.

Mr. Shedd. To me, I have looked at the deal with TikTok and ByteDance, which is the parent of TikTok, and the arrangement of a 20-percent, or 19.5-percent, ownership by ByteDance still of TikTok. Being able to carry out what was the mandate of Congress in closing down TikTok would be a great step forward.

It would do a couple of things. It would obviously cut off the access to data, but, by extension -- and my witness colleagues may speak to this more in terms of malign influence -- the ability to control the clicks associated with it.

But it would also signal to the Chinese that that is an unacceptable platform to have in the United States, of which there are 170 million users and 1.7 billion globally. And that would be one action, but would be taking the action that Congress and the mandate that Congress gave to that in shutting it down.

Chairman Moolenaar. Thank you.

Mr. Lucci, given the CCP's whole-of-society mobilization through its United Front strategy, how can we help Federal, State, and local partners address PRC-linked activity that exploits U.S. openness?

Mr. Lucci. Chairman, I think that what States could use a lot more of is expertise from the Federal Government about what these operations look like.

So they are dealing with things ad hoc. They see very strange activities in statehouses. They see the Chinese diaspora being targeted in places like Houston. And it is a new problem for

them to deal with.

I have spoken with law enforcement at the State level on the issue of, say, transnational repression, and what they will say is, "We know it is a real thing. When people talk to us about it, we know it is happening, we know it is likely a state actor behind it. But we have really, kind of, never trained on this stuff, as you would train on any number of other issues in your law enforcement training."

And so that is the type of thing -- I know that there are proposals on transnational repression from this committee and others -- that could help State leaders understand from a national-security, Washington, D.C., level what to understand and look for in these threats and how to counter these threats so that they are not, kind of, having to deal with it ad hoc as they see and learn about it in process, that they could actually train on it and learn about.

Some States -- Utah, Texas, and otherwise -- are creating their own training modules to counter transnational repression, but I think that they would all seek Federal expertise on that issue.

Chairman Moolenaar. Thank you very much.

And now I would like to recognize Ranking Member Khanna for 5 minutes of questions.

Mr. Khanna. Thank you, Mr. Chairman.

Mr. Lucci, a few months ago, you tweeted out, quote, "Two Chinese-Americans accused of attempted bombing at MacDill Air Force Base gained US citizenship via birthright. They are not loyal to the USA. There are 1,500,000 more 'Chinese Americans' essentially born in Saipan" -- which is a U.S. territory -- "and raised in Communist China. Denaturalize them all."

I would like to offer you an opportunity to correct the record for such a bigoted and xenophobic statement.

Do you believe millions of Chinese-Americans who gained citizenship through birthright should be denaturalized, or are you simply a racist?

Mr. Lucci. Congressman, what I am referring to are Chinese folks who are just born in a U.S.

territory and then go immediately back to China, they live their whole life in China. The estimate of 1.5 million comes from a book that came out --

Mr. Khanna. I am just asking you a simple question. Do you believe these people should be denaturalized? It is U.S. law that anyone born in a U.S. territory is an American citizen. Do you believe that 1.5 million should be denaturalized?

Mr. Lucci. I think that if they are loyal to the Chinese Communist Party --

Mr. Khanna. I am not asking you that. I am saying, they are born here. Do you think they should be denaturalized? One-point-five million.

Mr. Lucci. Congressman, I understand under the current laws that they have citizenship, as you are --

Mr. Khanna. And you think that should be changed?

Mr. Lucci. I think that if they have practically zero nexus to the United States of America, other than they were born in a territory, I think it is worth considering that, yes.

Mr. Khanna. Do you believe Chinese-Americans are more disloyal than other Americans?

Mr. Lucci. Congressman, there are seven Chinese-Americans who live in my household. I do not think that they are more disloyal than other --

Mr. Khanna. So you just think that they should be denaturalized even if they were born here?

Mr. Lucci. If -- so there are two types of issues we are talking about here. There are folks who are born here that are just raised here. They are Americans, like you and I. It is a very different thing when you have folks -- my understanding is about 50,000 per year are just born in a territory, they are there for a couple of weeks, and then they go back and they are raised in China. I think that the second --

Mr. Khanna. You are saying 1.5 million?

Mr. Lucci. Right. There are 50,000, and then you add it up over years, 50,000 to 100,000

per year. It is going on 15 to 20 years of this.

So I think that -- I actually think that this is a very clear security threat, because we have seen this -- so there is a gentleman --

Mr. Khanna. Are you saying this for -- so are you saying any American born here who then goes to a foreign country and is raised there should be denaturalized? Is that your position?

Mr. Lucci. That is not my position.

Mr. Khanna. Well, what is your position, then?

Mr. Lucci. When the Federal Government defines adversaries -- which the Federal Government does -- and then the Federal Government says, these adversaries pose a national-security risk to us, and then when you have --

Mr. Khanna. But you are not talking about -- you are talking about a blanket statement. You are saying, basically, in your tweet, you say -- and I can't believe you are not walking it back. I fundamentally find it fundamentally racist, and I don't use that word -- I don't think I have used that word in 10 years in a committee hearing.

But the reality is that you are basically saying that if you are Chinese-American and you are born under U.S. law in a territory, you should be denaturalized.

And I am asking you, does that just apply to China, or are you saying anyone who is born in a U.S. territory, if they then go to live in another country and are there, raised until 18, that they should be denaturalized?

Mr. Lucci. Congressman, let me restate. My household has eight people in it --

Mr. Khanna. I don't really care about your household. That is like saying, "I am friends with someone who is Black" but I am still a racist. I want to know what your actual policy is.

Mr. Lucci. Congressman, you accuse me of racism against my own family.

Mr. Khanna. Yes. I do. I think you are a racist. I think you are a racist.

Mr. Lucci. So you are accusing me of racism --

Mr. Khanna. I am not accusing you; I am saying --

Mr. Lucci. -- against my wife, my children --

Mr. Khanna. -- the actual statement. I think your statements are racist against Chinese-Americans.

And I am trying to understand whether you believe that this is just Chinese-Americans who should be denaturalized or whether you believe that anyone born here who goes to a foreign country and is raised should be denaturalized.

Mr. Lucci. The second part, certainly, that is not what I said. What I said was that, when folks are born in a territory, there for a week or two, they go back to Communist China, they have no real nexus to the United States of America, that we should consider that.

I think that that -- it creates a clear -- so take, for example --

Mr. Khanna. But are you saying that just for Chinese-Americans? Or anyone born in the United States who goes and is raised in a foreign country should be denaturalized?

Mr. Lucci. I would consider it for foreign-adversary nations, as defined by the Federal Government. That is where the Federal Government --

Mr. Khanna. So you want to denaturalize Iranian-Americans, you want to denaturalize Russian-Americans, you want to denaturalize Korean-Americans -- North Korea. I mean, where does this end?

Mr. Lucci. Congressman, when folks have no -- my point was, in the number of 1.5, obviously there are way more people of Chinese descent born in the United States of America, birthright through that. One-point-five is the estimated number of people born just in a territory, they are there for a very short amount of time, and then they are raised in China, loyal to the Chinese Communist Party. I think that that is a clear security risk.

But I will repeat: I take, you know, direct offense. You are saying I am racist against my own family.

Mr. Khanna. I think you are racist towards --

Mr. Lucci. My family is largely of Chinese ethnicity.

Mr. Khanna. -- Chinese-Americans. Yes, I do.

Mr. Lucci. Congressman, with all due respect, I think that is --

Mr. Khanna. We will put out this exchange, and the American people can decide, when you are talking about eliminating birthright citizenship for Chinese-Americans, whether they think you are a racist. I think a lot of Asian-Americans and many Americans will think you are.

Mr. Lucci. I think that, when people see that I have a Chinese wife and four Chinese children --

Mr. Khanna. I don't think that excuses racism.

Mr. Lucci. -- I don't think they are --

Chairman Moolenaar. The gentleman's time has expired.

Mr. Lucci. I don't think they are going to see racism in that, sir.

Chairman Moolenaar. Representative Johnson.

Mr. Johnson. Thank you, Mr. Chairman.

My line of questioning will be for Mr. Shedd.

Of course, one of the reasons that we know the American economic system is superior to that of China is that, by and large, the priorities and the market conduct of our companies are determined by managers and owners as opposed to government officials.

Now, of course, that being said, I do understand the real value that comes from properly constructed export controls and other IP protections. But I just want to chat with you a little bit about, how do we strike that right balance? How do we get the Goldilocks spot?

I think a number of members of the committee have been properly captivated by your "crown jewels" doctrine. How do we ensure that we don't overstep with the regulations around American company behavior? And are there some things that we should endeavor to not do as we attempt

to make sure that companies in America, that their interests are well-aligned with our national-security interests?

Mr. Shedd. Thank you very much for your question, Congressman.

I am struck by, as someone who grew up for a period of time in Chile under communism, 1970 to late 1972 -- and I can tell you, it wasn't --

Mr. Johnson. I am sorry. Perhaps the gentleman could pull the microphone just a little closer.

Thank you.

Mr. Shedd. Is that better?

And having grown up in Latin America and in Chile during that period of time, it is not a world that I want to live under, having state control of the private sector.

So, to your premise, how do we find that sweet spot, that Goldilocks perfect state, I would give you three ideas.

The first is encouraging corporate America -- and I don't mean legislatively but, certainly, as my colleague to the left has talked about, better educating what the Federal Government knows the Chinese are doing to corporate America, to be able to have them protect those crown jewels, as I refer to them, in what I call a "small yard with high fences" -- that is, the cyber protections around that. That may not be 80, 90 percent of the rest of the company, but where that IP is that they do not want to lose, that needs to be very clearly defined.

Secondly, I would look at the area of investments by China in the United States and the front companies that they set up, in terms of whether it is venture capital or into private equity, and where they own a piece of the company that they are a part of. And, again, I would encourage that my former colleagues of the Federal Bureau of Investigation have those kind of discussions at a higher level.

And, finally -- and, again, it is not a legislative action -- and I have spoken to a number of the

Fortune 500 chief security officers as a result of this book -- that security be elevated into the C suite, if I can put it that way -- in other words, treating it as it should be in terms of the threat that it represents.

But I am not here to argue that we are better off if the Federal Government introduces more legislation, more regulatory demands on most of corporate America, but, rather, that it be an education process in which they are able, then, to take the actions themselves -- motivated, by the way, by quarter-on-quarter profits that are affected by the stealing of their intellectual property.

Mr. Johnson. So, yes, I think the way you laid that out provides me more confidence. When you talk about educating and encouraging companies to do the right thing, I think that makes sense.

You know, in your testimony, you talked about requiring companies to treat their R&D and intellectual property as national-security infrastructure. Give me an example of what -- what form does that requirement take?

Mr. Shedd. So, coming out of an intelligence and defense background, I look at the listing of which you have a known affiliation by the Chinese, whether it is intelligence, security, or PLA in terms of its support -- which is virtually indistinguishable -- that has a relationship with Department of War contracts. There, you need to call that out. That is regulatory.

And so you would be identifying that list of those companies that have that association. And, frankly, when that is identified, if there is a merging of contract money that the taxpayers, the U.S. taxpayers, are putting into it with known Chinese association on the other side, that needs -- that is the regulated part. That is one example.

Mr. Johnson. Thank you.

Mr. Chairman, I yield.

Chairman Moolenaar. Thank you.

Representative Castor.

Ms. Castor. Well, thank you, Mr. Chairman.

Thank you to our witnesses today.

Mr. Shedd, thank you for your decades of service to the country, especially our national-security and intelligence agencies.

In your book, "The Great Heist: China's Epic Campaign to Steal America's Secrets," you delve deeply into the ways that the CCP has malign designs and steals America's intellectual property. And you have just given us a few pieces of advice, to not overdo it from a legislative perspective, but, in your testimony, you mentioned that we need to prosecute these thefts more effectively.

Do you have any explicit recommendations for us on how we really hold the CCP accountable for their theft of IP?

Mr. Shedd. I think the tone is set at the top -- and when I say that, I mean the White House and the Department of Justice -- in looking at cases where the prosecutors are somehow incentivized to prosecute known espionage -- this isn't about profiling; it is about the facts of that activity -- in a way that -- I am not sure that my former colleagues at the FBI think of the Chinese economic espionage in the scale that it represents -- and the ability, then, to prosecute them, with an understanding that -- for example, building a witness capability, where a number of those witnesses have either fled back to China, against a now-clear case in terms of the prosecution, there ought to still be a way to bring a conclusion to that prosecution in that manner.

And, secondly, I think it is back to the education and the direction from the top. The scope, the size, the depth of what the Chinese are doing is so broad and so wide that I think our DOJ needs to think more proactively about how they stem that through the process of prosecutions.

Ms. Castor. Yeah. And part of -- I have been concerned with the mixed messages coming from the top of the administration when it comes to what the CCP is doing. And the Office of the Director of National Intelligence has been in the news lately and over the past year for sure, and last year they scaled back the Foreign Malign Influence Center. That seems like that would be

particularly counterproductive to American interests when we are trying to counter what China -- what the PRC is doing to steal our intellectual property.

What is your view on the scaling back of the Foreign Malign Influence Center that was intended to take on these threats?

Mr. Shedd. Without having any insights as to how effective it was, clearly, on the surface of scaling it back is a mistake.

Not only has that malign influence continued -- it has continued to grow, as I gave the example of TikTok as an example of the capabilities of having a platform -- but you have the Confucius Institutes. A hundred, I believe, is the number inside the United States. And understanding what they are doing -- now, I am not arguing that that ought to be a CIA or DIA mandate, but it should be an FBI mandate.

And so scaling that back, to me, without knowing the details of why and how that decision was taken, is, at its core, a mistake.

Ms. Castor. Raises red flags to me.

Mr. Yang, in your testimony, you state that American greatness was built on the students who came to study at American universities and stayed to build American companies, researchers who collaborated across borders and advanced American science and business relationships.

Particularly in the context of academic research, what types of research security policies do you think would be helpful at this time?

Mr. Yang. Well, thank you for that question.

Certainly, one favorable development that we have seen is the implementation of what is called NSPM-33. So this is a directive that was initiated by President Trump and carried through by President Biden that really standardized how disclosure forms work with respect to Federal grants through the NIH or other Federal grants for science and research.

One of the problems that researchers encountered was, there was a patchwork of different

disclosure requirements. They did not understand them. Oftentimes, they violated it. And, frankly, what we saw were that Asian-American scientists and researchers got targeted because of these types of violations. By standardizing these conflict-disclosure forms, now we actually can get some more transparency as to what is happening.

And each university -- this is where I would agree with Mr. Shedd, education is important -- is, universities should be educated about what are the actual conflicts, what are the pain points, the security points that we should be aware of, so that we can address them in a very precise way rather than over-generalizing.

You are absolutely right with respect to researchers. One thing that should be noted: There have been studies done by the Migration Policy Institute and Asian American Scholar Forum that shows that approximately 75 percent of all foreign scientists stay in the United States.

That says something about the contribution that foreign scientists give to the United States. So part of this is, how do we make sure that we keep them here to allow them to innovative and continue to grow our economy?

Ms. Castor. Thank you.

I yield back.

RPTR SCHWALM

EDTR HOFSTAD

[11:32 a.m.]

Chairman Moolenaar. Thank you.

Representative Bilirakis.

Mr. Bilirakis. I am not sure if this thing is on or not. Okay, it is working.

Okay. Thank you very much. Thanks for holding this hearing, Mr. Chairman.

I do have quite a few questions here, and I know I have a limited amount of time, but I do want to give Mr. Lucci an opportunity to respond at the accusation that one of my colleagues made with regard to him possibly being -- I don't believe this, but -- a racist.

Please, but briefly, sir --

Mr. Lucci. Congressman, thank you.

Mr. Bilirakis. -- I want to give you the opportunity.

Mr. Lucci. I think that there are real policy issues to discuss here: what immigration looks like, who we let go near military bases, and furthermore. That policy debate is destroyed when someone is accused of being racist against their own children. It is absurd. It makes zero sense.

Policy is policy, but the whole conversation gets destroyed if we just throw the race card around against people -- as I said, my household is a big household. We have eight people. I am the only one with no Chinese ethnicity in my entire household.

So, for the Congressman to say that I am motivated by racism against my own wife, my own children, my own in-laws, it is completely absurd, and it destroys our ability to come to real policy solutions.

We should avoid this type of, you know, "race card about everything." Let's have a policy conversation, because this is a very, very serious threat we face from the Chinese Communist Party.

Thank you.

Mr. Bilirakis. Thank you. Agreed.

Mr. Shedd, you briefly mentioned in your written testimony the challenges of managing the modern threat of legal Chinese acquisition of American companies with sensitive technologies, customer data, or IP.

How does the intelligence community currently assess that risk? And how does that assessment compare if that information was transferred via a cyber breach?

Mr. Shedd. Thank you for your question.

Again, while I still hold my clearances, I am not in the day-to-day business of the intelligence community to give an opinion on that.

Certainly, what I understand the intelligence community position to be, though, is that that risk is still very high, in response to your question, and that the moderation -- or the modification that the Chinese are doing now -- and when I say "the Chinese," I am referring to the CCP -- is to Made in China 2025, which has launched in 2015 -- now has been extended to 2030.

And we know that, within that plan, they have two very high priorities of focus -- one is aerospace, and the second one is biotechnology -- because they did not meet their goals, out of the 12-ish or so of those goals, within Made in China 2025.

And so that is where I would place that.

Mr. Bilirakis. Thank you.

I am going to go to the third question, because I know I don't have much time.

Mr. Shedd, when the intelligence community identifies foreign nationals with potential strategic intent to acquire sensitive U.S. intellectual property or technology through transactions that fall outside the CFIUS jurisdiction, what mechanisms exist, if any, for communicating relevant risk information to policymakers or the private sector prior to deal completions?

Mr. Shedd. Thank you for that question, which is a profoundly complex one to answer, because the intelligence community as a whole has not focused, as the Chinese have focused, on

economic intelligence -- or economic espionage and intelligence by extension.

And so, understanding the CFIUS process and what is behind that -- of which I was a member of when I was still in government -- in reviewing that, I think it is critical to be able to get economic and financial intelligence from the Chinese as a collection matter in order to be better informed to understand what the ultimate objectives of that particular CFIUS review process is when it comes to the foreign-investment-related that could present a -- not necessarily dispositive, but could present a national-security threat to the United States.

Mr. Bilirakis. Thank you very much.

And, again, Mr. Lucci, I don't believe you are a racist, and I know how much you love your family.

So thank you very much, Mr. Chairman, and I yield back.

Chairman Moolenaar. Thank you.

Representative Carson.

Mr. Carson. Thank you, Chairman and Ranking Member.

Mr. Lucci, many States have passed laws targeting direct Chinese land purchases or investments near sensitive sites. Do those laws reach Chinese-controlled entities operating under American brand names?

And can a Chinese-owned company that presents as an American employer lobby State legislators, accept economic development initiatives, or influence State procurement without triggering any disclosure requirements?

Mr. Lucci. Congressman, you said "without triggering" -- I missed the last few words there.

Mr. Carson. Triggering disclosure requirements.

Mr. Lucci. Congressman, thank you.

In terms of the purchases of land, usually that is determined by who actually owns the entity. So, if it is an American subsidiary, for example, Cirrus Aircraft, which was recently blacklisted by the

Pentagon because they are ultimately owned by a Chinese military company, and so purchases by Cirrus would be subject to such laws.

I will give you one example. Cirrus just blocked a critical-infrastructure protection in Florida because it would have impacted them and their access to critical infrastructure in the State.

In terms of economic incentives, actually, again, Cirrus was supporting a law in Tennessee to give themselves economic incentives for being in Tennessee. It is very normal for foreign-adversary companies to benefit from economic incentives at the State and local level, perhaps at the Federal level as well. I don't look at that as much.

There have been States -- Nebraska and otherwise -- who have cut off those economic tax incentives to foreign-adversary companies, whether China, Russia, Iranian, or otherwise.

In terms of disclosures -- so some States have done foreign-agent laws. Those will also tend to look through and say, who is actually behind this company? And, again, the companies -- say, for example, Smithfield -- American name, but it is owned by China -- Smithfield would be impacted by a foreign-agent-registration law at the State level.

And, in fact, that is the company that issued a veiled threat to Nebraska State Senator Eliot Bostar for advancing a foreign-agent bill in Nebraska. They went to his office and they talked about economic disruptions to the State if that bill were to advance.

Thank you.

Mr. Carson. Yes, sir. Thank you.

Mr. Shedd, you spent 33 years in intelligence. Thank you, sir. Please help the committee understand this.

If China hacked an American company and walked out with customer data, manufacturing secrets, and even R&D, we would have the FBI at their door. And I come out of the IC.

But if they buy that same company through a legal acquisition and they get all of that and more with a handshake and a press release, is our government effectively treating those two

scenarios as equally dangerous? Or does legal paperwork give us kind of a blind spot that we can afford to overlook?

Mr. Shedd. Well, thank you for that question, and thank you for your service in the IC.

I do believe that there is a blind spot with that, and it has to do with all the very legal means in which Chinese investment is being done in the United States, whether it is at the venture-capital level into private equity or directly in terms of what they are buying.

So, as you say in your scenario of the first case, it would be treated as economic espionage if it were taken out. But then buying the company and then having that intellectual property and the rest of the knowledge and the capability associated with it would be under a legal framework.

And so I think that is an area that needs to be looked at very, very carefully if we, again, can find that directive -- or that direction from the CCP and the Ministry of State Security as a security matter.

And that may not be all companies inside the United States, by any means. But, certainly, in your example, if it first was treated as economic espionage and they buy that exact same company, it sounds to me like there is a loophole that is available to Chinese buyers.

Mr. Carson. Yes, sir.

Lastly and quickly, Mr. Yang, you have documented how the China Initiative devastated careers of innocent scientists -- people who made minor disclosures and even errors but not espionage, as it were.

I want to ask you the harder question, sir. Do you believe that there is a way to aggressively target genuine CCP infiltration of university research, the kind of partnerships that Mr. Lucci describes, while fully protecting Chinese-American students and faculty from being treated as suspects?

Mr. Yang. I think there is a way. There is a couple of things that I would suggest.

Number one, like I said, NSPM-33 is a start, because it provides for the disclosures that are

necessary to identify real conflicts of interest.

Number two, I would offer that we should make sure to educate universities on the types of conflicts that are involved, the sensitive technologies that are involved, so that we could understand what areas we all need to be clear on.

Similarly for FBI and law enforcement, making sure that they are educated about what constitutes open research that is part of the research world versus what constitutes actual national-security threats.

Lastly, I would want to incentivize to make sure that those researchers that want to be here -- most of them come here because they want to be here -- have the means of doing so.

One area I think that there is agreement is, this includes reform of our immigration laws to make it easier for them to become citizens here, reform of our immigration laws so that they could bring their family members here so that they would not be subject to that transnational repression that we are talking about.

Mr. Carson. Thank you, sir.

I yield back, Mr. Chairman.

Chairman Moolenaar. Thank you.

Representative Gimenez.

Mr. Gimenez. Thank you, Mr. Chairman.

And, Mr. Lucci, I am going back to what my colleague went back to, and I also believe that you are not a racist. And I just want to ask you again: Members of your family -- your wife, where is she from?

Mr. Lucci. She is from -- she was born in Tianjin, China. She came here for graduate school.

Mr. Gimenez. And I guess -- so that makes your children will be, you know, half-Chinese. Your in-laws are also Chinese?

Mr. Lucci. They are, yes.

Mr. Gimenez. Thank you.

And so it kind of makes it -- I understand now why one of my colleagues was cutting you off. Because the answers would be a little bit inconvenient to a charge of racism when, in fact, your household is mostly made up of Chinese-Americans.

Mr. Lucci. Congressman, it is as if I would be called anti-Italian, even though I have Italian ancestry, because I simply criticized the mafia.

Mr. Gimenez. I gotcha.

Mr. Lucci. I think that Italians can criticize the mafia --

Mr. Gimenez. Yeah.

Mr. Lucci. -- without being anti-Italian.

Mr. Gimenez. Correct. I understand.

And then it is easy to cut you off and say that you are a racist, and then anything that you would say will be discarded because you are, in fact, a racist, right? I mean, that is the whole point of the questioning.

Now, do you know where I am from?

Mr. Lucci. Congressman, I believe you are from southern Florida?

Mr. Gimenez. Nope, but do you know where I was born?

Mr. Lucci. Cuba?

Mr. Gimenez. I was born in Cuba. You know, I came here when I was 7, all right?

You know who I am loyal to?

Mr. Lucci. Congressman, I assume it is the United States of America.

Mr. Gimenez. I am loyal to the United States of America. And I stayed 6 years in -- 6-1/2, almost 7 years in Cuba. I am loyal to the United States of America. I am certainly not loyal to the Communist Party of Cuba.

And so I understand your reasoning that somebody that comes here for 2 weeks and then lives their entire life in China may not be loyal to the United States of America, because I am not loyal to the country of my origin. I am loyal to the United States of America.

Would it surprise you to know that -- and, by the way, I support birthright citizenship. I do. Okay? But you also have to understand that there are variations of that -- all right? -- and that we have to be smart as we protect American security.

And so would it surprise you that China does not have birthright citizenship?

Mr. Lucci. Congressman, my understanding is that our birthright citizenship is quite unique amongst the world.

Mr. Gimenez. Right.

But would it also surprise you that, as soon as you, as a Chinese national, then go out to another country and get a -- be a citizen -- try to be a citizen of another country, you know what happens to you? You lose your Chinese citizenship, automatically.

Did you know that?

Mr. Lucci. Yes, Congressman.

I think an important point to add on to that is: The Party doesn't care if a Chinese-ethnic person is an American citizen. The Party still considers Chinese-Americans subject to their rule. They just -- an ethnic unity law is going into effect July 1 of this year, and the Party says that it gives them more power to go after anyone in the United States with any Chinese ethnicity.

So the Party doesn't care what your citizenship is. They are the ones who focus everything on race. If you have any Chinese ethnicity, the Party says they get to go after you.

Mr. Gimenez. I understand. And I don't want to be like the Communist Chinese Party, okay? I don't want America to be that.

But I understand the reasoning that, hey, we may have to look at those folks that have been spending all their life in China, that may have American citizen- -- maybe a little bit different, maybe.

Okay? Because it is just -- I can see myself, all right? Like I said, I am loyal to the United States of America. I am not loyal to Cuba, even though I was born there and stayed 7 years there.

Going off that, I believe that there is a pattern that is developing of attacking AI. And I believe that there -- you know, I guess the suspicious nature of me says that somehow the CCP is involved in this because they want us to stop doing what we are doing so that they can win the race to AI.

Am I far off in my thinking, Mr. Shedd?

Mr. Shedd. I think you are spot-on.

In the race for artificial intelligence and who is going to come out ahead, they have every vested interest to create conflict in the United States and -- I think the term -- "sow discord" in the United States over data centers and everything that is associated with that.

And their goal is ultimately to merge ahead using all tools available to them in order to create this friction point, which is beginning to emerge in a very, very decided way in terms of the political implications and all of that.

They then combine that with -- they mix it up with the issues of the electric grid and all the rest of the other aspects of it.

No, that is not a coincidence.

Mr. Gimenez. And I think they are using that for their advantage and to try to put an anchor around our research into AI, because they understand how critical it is for us to win AI, for them to win AI, because, frankly, it is the future.

Finally -- I don't know how much time I have left, but one final question.

We have a number of large corporations that operate out of China, and I know that there are laws that say they must cooperate with the PLA and Chinese intelligence agencies.

Some of these large corporations have been telling us that, no, they don't; they don't comply with that.

I don't know who can answer this, but do you believe those large corporations? Or do you believe that they are just telling us that so that we allow them to remain there?

Because I actually believe it is a huge security risk for the United States for those large corporations and their intellectual property to be in China and actually cooperating with Chinese authorities.

Mr. Shedd. Every one of those corporations that operate in China have CCP employees, hard stop. That is just the reality of it. They have a duty to report and collect on that company.

Secondly, every U.S. corporation that is -- or Western corporation that is vested or invested in China does not have control of its cyber capabilities within the mainland. Those belong to the Chinese Communist Party.

Thirdly, every one of those now is affected by new laws that have been passed since 2015 -- the Cybersecurity Law, in which the data then that they intend to extract is prohibited from being taken out. Their profits are now being affected in terms of what they can remove.

And the most nefarious is the National Intelligence Law that was passed in 2018, and that is Article 7, in which every Chinese citizen, when called upon -- and that is an important point to underscore -- when called upon, must cooperate with the Chinese Communist Party through the mechanisms of the Ministry of State Security, both at the provincial level and all the way up to their version of the Federal level.

Thank you.

Mr. Yang. If I might, if I could have the opportunity, since I served as legal director for an American company, Illinois Tool Works, in China, I will say that there are manners in which our company was able to manage our intellectual property, manage our trade secrets in a manner that would protect our company and protect our innovation in remaining in the country.

I agree with Mr. Shedd that there are challenges to all of that and there is an evolving network. But I think this is where I would agree with him, that education of our companies is so

vital to this, because there are manners in which we can do this, but it requires cooperation, it requires education, it requires a level of expertise that sometimes we are just being a little bit too simplistic about.

Chairman Moolenaar. Representative Tokuda.

Ms. Tokuda. Thank you, Mr. Chair.

You know, as the great-granddaughter of a Japanese-American who was imprisoned during World War II, I am acutely aware that some of our worst violations of civil liberties in our Nation's history have been carried out under the banner of national security. And, looking back, we know that criminalizing an entire community, you know, made Americans not stronger or safer but actually weaker and more vulnerable.

We must ensure that our response to Chinese espionage does not repeat the egregious mistakes of treating people as suspicious because of their ancestry rather than because of the evidence at hand.

Mr. Shedd, can someone born in the United States be disloyal to America? Just say "yes" or "no."

Mr. Shedd. Yes.

Ms. Tokuda. Can someone who lives their entire life in the United States be disloyal to America, yes or no?

Mr. Shedd. Yes.

Ms. Tokuda. Can someone who is not of Chinese descent be loyal to China, yes or no?

Mr. Shedd. Yes.

Ms. Tokuda. So, you know, we are a country that tends to be focused on classifying by race, but if we look at the ODNI and the FBI China threat investigation, Chinese intelligence agencies do not use race or ethnicity as a primary criteria for their recruitment. They instead focus on specific access clearance or expertise of an individual.

We also know that a significant share of known espionage cases involve non-Chinese operatives.

If we are focusing so much of our suspicion on people with a particular ethnic background, aren't we effectively looking in the wrong places while creating the very kind of fear and distraction and division that our adversaries and their propaganda seek to exploit?

Mr. Shedd. I assume that question is directed at me?

Ms. Tokuda. Uh-huh.

Mr. Shedd. I think both things can be right at the same time, "both things" being: There is this imperative by the Chinese Communist Party to use ethnic Chinese in terms of access that they may have -- and that is not to say that they are all spies, by any means or any stretch of the imagination.

However, on the other hand, there are clearly non-Chinese who have spied on behalf, including from my former agency, the CIA. And we know those cases -- they are now public, because they have been prosecuted -- in which the Chinese targeted them in order to get access to, as you referred to it, classified information and all of that.

The storyboard of "The Great Heist," though, is largely focused on how the Chinese go after their targets and they will use whatever means is available to them. And I don't believe they do it strictly off of ethnic profiling on their part but, rather, what is the requirement that they need to meet.

On the other hand -- and I think the words were used in terms of -- from the Chairman -- the access, the coercion, and then the incentives. The Chinese Government, the CCP in particular, pushes those three lines of effort against those who they have the greatest part of their access to. And that would be Chinese-Americans or Chinese -- and, again, that is what -- it has to be looked at that way, because that is how they are leveraging it.

Ms. Tokuda. And I understand that. But I do feel that we are creating a self-imposed blind

spot here by simply classifying vulnerability, potential for coercion, based upon one's ethnicity.

Quite frankly, China's Government wants Americans to believe that competition with the CCP is not competition with them but with people of Chinese descent. If we are going to allow ourselves to blur that distinction, quite frankly, I think we are handing them a propaganda victory, and, simultaneously, we are undermining the trust and cooperation that we need for effective counterintelligence measures as well.

You know, right now -- and this will be my last question, Mr. Chair; I know I am running over time -- press reports are indicating that the ODNI is working to take over counterintelligence.

This is where we need to have that trust. We need to be able to effectively have allies on our side to let us know what is going on. But the DNI is working to take over counterintelligence responsibility from the FBI.

And given that the new Acting Director, Bill Pulte, has zero experience in intelligence, zero experience in counterintelligence, zero experience, quite frankly, in national security, if China is truly, in fact, our urgent and growing threat, aren't we just handing them a huge window of opportunity, especially given China's reliance on pushing the propaganda that we are simply looking at Chinese descent and Chinese-Americans and Chinese researchers and scientists and companies versus actually, in many cases, the operatives that they are recruiting based upon their access, based upon their experience, all of these things? Which, in many cases, a significant number of these operatives are not, in fact, of Chinese descent at all.

Mr. Shedd. Thank you for your question.

And I agree that the capabilities of counterintelligence ought to stay with the professionals, and that would be the FBI. They have a long history of running counterintelligence operations.

In the second half of your question and commentary that I agree with, as well, is that the Chinese want to foster this division around race, among many other reasons in terms of creating discord. So it is a propaganda benefit to them to generate that kind of image that we are doing it

on the basis of race profiling.

Ms. Tokuda. Thank you, Mr. Chair.

And just in closing, I would just remind people that we have been in this place in history many times over, as has been brought up, whether it is the Chinese Exclusion Act, whether it is the internment of Japanese-Americans like my GG, my great-grandfather.

We need to start to learn from the mistakes that we made -- that if, in fact, this is about true competition, if, in fact, this is about taking out our adversaries before they spy on us, then we have to learn from the mistakes of our past and not judge people by the color of their skin or where they were born but, in fact, take a look at the evidence and really be able to make sure that we are running intelligence intelligently.

Thank you, Mr. Chair. I yield back.

Chairman Moolenaar. Thank you.

Representative Stanton.

Mr. Stanton. Thank you very much, Mr. Chairman.

Thank you to the witnesses for being here today.

Our national-security agencies play such a critical role in countering foreign malign-influence operations from the PRC.

The Office of Director of National Intelligence and the State Department had offices dedicated to monitoring and combating foreign influence, called the Foreign Malign Influence Center and the Counter Foreign Information Manipulation and Interference Hub, respectively.

Unfortunately, this administration shut those offices down. In doing so, this administration dismantled the last remaining Federal Government offices dedicated to tracking and analyzing malign-influence operations that harm U.S. national interests.

And just this week, dozens of career intel officers were let go by Acting Director Pulte, further eroding the expertise needed to tackle these critical issues.

At a time when Congress is demanding answers as to what our government is doing to counter foreign malign influence, this administration has clearly taken a step in the wrong direction.

Mr. Shedd, how does the loss of dedicated resources and expertise across our national-security agencies create vulnerabilities for the United States?

Mr. Shedd. Thank you for your question.

Clearly, I care passionately about being able to counter the malign influence. Losing professionals that I worked for for the better part of almost three and a half decades as a result of whatever decisions are being made in the administration, and particularly in the intelligence community that I so much love and respect, has the effect of really tearing down the capabilities that ought to be built up at a very critical time.

Now, is there an opportunity, at the same time -- this would have been my approach, is, let's look at the effectiveness of those efforts within these offices. Were they really being as effective as they should be?

That is a very different question and then outcome than simply saying we are doing away with that office notwithstanding what we see as this enormous line of threat that we face.

Mr. Stanton. Yeah. I think we are agreement that those offices should have stayed open. They could always be improved, but work on always improvement.

Shifting gears, IP theft. The FBI has found the annual cost to the U.S. economy of counterfeit goods, pirated software, theft of trade secrets to be between \$225 billion and \$600 billion.

Several Chinese companies that the U.S. Government has formally designated as national-security threats, including Huawei, BOE Technology Group, and Tencent, rank among the top recipients of U.S. patents, receiving thousands each year. These companies have used these patents to sue American firms, transfer rights to patent trolls, and, as in the ongoing YMTC v. Micron case, compel disclosure of sensitive trade secrets through discovery.

Mr. Shedd, should entities that our own government has flagged as national-security risks continue to receive U.S. patent protection that they can turn around and use as a weapon against American companies?

Mr. Shedd. Thank you for that question.

And the answer is, absolutely not. It is beyond just a paradox that that would occur once you have that evidence that you cited in those examples. And I find it highly disturbing that that is allowed to happen, that the very companies that are part of the threat are allowed to turn around and sue as a result of having those patents.

Mr. Stanton. Thank you very much.

One final question.

Mr. Yang, in your testimony, you state, American greatness was built on, quote, "students who came to study at American universities and stayed to build American companies, researchers who collaborated across borders and advanced American science, and business relationships that gave both countries a stake in the other's stability."

Mr. Yang, how do we ensure that, while being attentive to real national-security concerns, we continue to make sure our country is a place where talent from all over the world continues to come to study and work?

Mr. Yang. Thank you for that question.

I think there are two things that are important.

One is just rhetoric. I am very concerned when I hear categorizations of an entire group of people as "foreign adversaries." Yes, the Chinese Government is a foreign adversary, no question about that. But when we say that the people are foreign adversaries or that is how it is defined in legislation, that becomes a problem.

Even with respect to Chinese companies, certainly there are Chinese companies that are state-run that present true national-security treats. But then there are also companies that are just

engaged in capitalism, like all of us.

Having rhetoric that says all Chinese students are spies, all Chinese and Indian immigrants are gangsters with laptops, or that we should have a China Initiative case in every jurisdiction in the United States are categorizations that lead to bad results.

Then, the second thing is making sure that we have policy that is narrowly tailored. We should use a scalpel, not a sledgehammer -- not engage in broad categorizations, but engage in the type of nuance that is necessary.

Mr. Stanton. Thank you very much.

I yield back. Thank you, Chairman.

Chairman Moolenaar. Thank you.

I want to thank all of our witnesses today. Very much appreciate your testimony.

Questions for the record are due 1 week from today.

[The information follows:]

***** COMMITTEE INSERT *****

Chairman Moolenaar. And, without objection, the committee hearing is adjourned.

[Whereupon, at 12:03 p.m., the committee was adjourned.]