

**STATEMENT OF WILLIAM R. EVANINA  
CEO, THE EVANINA GROUP**

**BEFORE THE SENATE SELECT COMMITTEE ON  
INTELLIGENCE**

**AT A HEARING CONCERNING THE COMPREHENSIVE  
THREAT TO AMERICA POSED BY THE COMMUNIST PARTY  
OF CHINA (CCP)**

**AUGUST 4, 2021**

Chairman Warner, Vice Chairman Rubio, and Members of the Committee — it's an honor to appear before you today. I have been honored to brief this Committee on a regular basis over the past decade as the Director of the National Counterintelligence and Security Center, and as a senior counterintelligence executive in the CIA, and FBI. I was tremendously honored to be the first Senate Confirmed Director of NCSC in May of 2020. I am here before you today a private citizen, and CEO of The Evanina Group, LLC. In this role I work closely with CEOs and Boards of Directors to advise on the issues we are about to discuss and develop strategic mitigation efforts to ensure effective defenses, as well as brand protection.

Today's topic, the holistic and comprehensive threat to the U.S. posed by the Communist Party of China (CCP) is as critical of a topic, and threat, as we face today as a nation.

I have spent 32 years of my adulthood working the U.S. Government. Twenty-four of which with the FBI, CIA, and NCSC.

Our nation faces a diverse, complex, and sophisticated threats by nation state actors, cyber criminals, and terrorist organizations.

Russia poses an increased, and significant intelligence and cyber threat to the US, in both the public, and private sectors. Vladimir Putin, with his aggressive intelligence services along with loyal, highly resourced oligarchs, continue to push boundaries in numerous geopolitical and cyber arenas. Putin's goal to destabilize the U.S. and degrade our Democracy in evident every day, especially in illicit cyber activity and extensive social media malign influence campaigns.

Iran and North Korea continue to pose a challenge to the U.S. particularly from a cyber perspective.

However, the existential threat our nation faces from the Communist Party of China (CCP) is the most complex, pernicious, strategic, and aggressive our nation has ever faced.

I proffer that the U.S private sector has become the geopolitical battlespace for China as a baseline for this comprehensive and nefarious behavior.

Xi Jinping has one goal. To be THE Geopolitical, Military, and economic leader in the world. XI, along with the China's Ministry of State Security, People's Liberation Army, and the United Front Work Department, drive a comprehensive and whole of country approach to their efforts to invest, leverage, infiltrate, influence and steal from every corner of U.S. success.

Economic security is national security. Our economic global supremacy, stability, and long-term vitality is not only at risk, but squarely in the cross hairs of Xi Jinping and the communist regime. It is estimated that 80% of American adults have had all of their personal data stolen by the CCP, and the other 20 percent most of their personal data. This is a generational battle for XI and the CCP, it drives their every decision, particularly geopolitically. How to counter and push past the U.S. is goal number one for the CCP.

Intelligence Services, Science & Technology Investments, Academic Collaboration, Research Partnerships, Joint Ventures, Front Companies, Mergers and Acquisitions, and outright theft via insiders and cyber intrusions, begin the comprehensive and strategic framework for how China implements their strategy.

China utilizes non-traditional collectors to conduct a plurality of their nefarious efforts here in the U.S. due to their successful ability to hide in plain sight. The non-traditional collectors, serving as engineers, businesspersons, academics, and students are shrouded in legitimate work and research, and oftentimes become unwitting tools for the CCP and its intelligence apparatus.

China's ability to holistically obtain our Intellectual Property and Trade Secrets via illegal, legal, and sophisticated hybrid methods is like nothing we have ever witnessed. Joint ventures, creative investments into our federal, state and local pension programs, collaborative academic engagements, Sister City Programs, Confucius Institutes on Campus, Talent Recruitment Programs, investments in emerging technologies, and utilization of front companies continue to be the framework for strategically acquiring the thoughts and ideas of our researchers, as well as development of those ideas pre and post patent application. The threat from China pertaining to academia is both wide, and deep. My colleague Anna Puglisi will discuss this more thoroughly today. However, the past three years of indictments and prosecutions have really highlighted the insidiousness of China's approach to obtaining early and advanced research as well

as understanding the complexity of gifts and funding at U.S. colleges and universities, particularly when tied to federal grants.

China's priorities for obtaining U.S. based technology and know-how, pursuant to their publicly available 25 Year Plan are Aerospace, Deep Sea Technology, Biotechnology, Information Technology, Manufacturing, Clean Energy, Electric Battery Technology, and DNA/Genomics. Any CEO or Board of Directors leading in any of these critical industries must become aware of the threat posed to them and work with their security team and outside experts to identify risk-based mitigation strategies.

The proverbial salt in the wound of all this nefarious activity is when the CCP steals our thoughts, ideas, patents, and technology, and manufactures that same technology in China, and then sells it back to American companies and around the world. One needs to look no further than the American Supercomputer Corporation for just a glimpse of the long-term impact to economic espionage. Then one must factor in all the manufacturing plants which were not built, and the tens of thousands of jobs which were not created because China, via its theft, beat the U.S. to the global market and is selling the same product and a significant reduction in real costs.

Boards of Directors and investment leaders must begin to look beyond the next fiscal quarterly earnings call and begin to think strategically with respect to how their decisions and unawareness of the long-term threat impact their businesses and industries, which is woven with our national security, economic stability, and endurance of our republic.

In 2017, the Communist Party of China issued new state laws to facilitate the perniciousness of their efforts to obtain data, from everywhere. Three specific portions of those laws should be understood, and be an enduring reminder to CEOs, General Counsels, Chief Data Officers, CIOs, and CISOs, throughout our private sector ecosystems.

The first is Article 7 of the People's Republic of China National Intelligence Law summarily stating that all business and citizens shall cooperate with China's intelligence services and shall protect all national work secrets.

The second is Article 77 of the same National Security Law summarily stating that Chinese citizens and business shall provide anything required or requested by the Chinese government or intelligence services.

The third is Article 28 of the 2016 Cybersecurity Law summarily stating that all network operators must provide data to, and anything requested by, national, military or public security authorities.

Hence, if you are a U.S. business seeking to enter a business relationship with a company in, or from, China, your data will be obtained and provided to the MSS or PLA for their usage. This includes third party data as well. The analogy is

a U.S. company enters into a business deal or partnership with a company from another country. The U.S. company must provide all relevant and requested data from their company, as well as the partner company, to the NSA, CIA and FBI.

Additionally, China plays by their own rules. China does not conform to any normalized set of regulations, guidelines, norms, laws or value-based agreements throughout the global economic ecosystem.

To further the Communist Party of China's unlevelled economic playing field, out of the 15 largest companies inside China, 13 are either owned by the CCP or run by the CCP. The world has seen recently what the CCP is capable of when one of the largest companies in the world, Alibaba, pushes back on state-run efforts.

American business leaders, and Americans in general, must understand that China is a Communist Country run by an authoritarian "President" for life. Unlike in the U.S. and Western Democracies, and like Putin's Russia, there is no bifurcation between the government, industry, and or criminal organizations.

Hence, for a prospective business deal with a company in the U.S., the Chinese company can partner with China's intelligence services to assist in negotiations, vulnerabilities, and utilization of any already acquired data from said U.S. company. Again, this is akin to a U.S. based company calling the CIA and NSA for assistance on preparing a bid to merge with a company outside the U.S. and use all types of classified collection to form a proposal or use during negotiations.

The willingness of China, and its intelligence services, to illegally, and legally obtain DATA to drive artificial intelligence, research and development programs, and to facilitate their military and economic goals without doing the hard work to independently develop on their own, drives at the heart of China's unfair practices.

From genomics and DNA to third party financial data stored in cloud services providers, to fertility to Internet of Things technology, the effort du jour is accumulation of data, and lots of it.

China continues to surprise the world by aggressively stifling their citizens via laws, regulations, unparalleled domestic surveillance, and a debilitating Social Credit Score for every citizen. And a conversation about what is occurring the Uyghurs is for another hearing.

China's efforts to prohibit and violate free speech inside the U.S. must be identified, exposed and mitigated. China conducts such activities on Chinese nationals and on American citizens. Similarly, the CCP utilizes a suite of capabilities to silence critics here in the U.S. when the activity is exposed. The utilization of the United Front Work Department to drive false narratives in social media and within mainstream print and television media is consistent and

enduring. There are numerous examples of such, however I want to reference just a few recent examples. The first is the Chinese Embassy in Washington DC pressuring Nobel scientists to censor their speeches at the 2021 Noble Prize Summit. The prize winners were bullied by the Government of China to disinvite the Dalai Lama for the award ceremony. The second example is Zoom executive charged for working with the Chinese intelligence services to disrupt Zoom calls in the U.S. commemorating Tiananmen Square. The third example is American actor John Cena apologizing, in Mandarin, because of the pressure Chinese officials placed on him, and Hollywood, because he referenced Taiwan as a country. The pressure being placed by China on Hollywood has grown to a credibility questioning level and impacts just about every decision they make with respect to scripts and potential villains. This is referred to as “apology diplomacy” and has been publicly visible for many years when CEOs and company executives must apologize to Xi or the China for indiscretions with respect to referring to Taiwan as an independent country.

The last example, I feel is the most disturbing effort by the CCP here on American soil. Operation Fox Hunt is an international effort by the CCP to identify, locate and attempt to bring back Chinese dissidents who have left China and are causing President XI and the Communist Party discontent. For almost a decade Chinese intelligence services have been building teams to conduct surveillance in the U.S., oftentimes falsely enter relationships with local law enforcement to garner information on who China claims are fugitives, and attempt to bring them back to China.

The willingness, ability, and success of the Communist Party of China to conduct such aggressive activity within the confines of America’s borders is disturbing and unacceptable.

From a cyber perspective, China has significant and unending resources to penetrate systems and obtain data, or sit dormant and wait, or to plant malware for future hostilities.

Just last week, the FBI unveiled details for the first time on a 2011-2013 Chinese state-sponsored cyber campaign against U.S. oil and natural gas pipeline companies that was designed to hold U.S. pipeline infrastructure at risk.

Additionally, in July 2021, DOJ unsealed an indictment charging four individuals working with China’s MSS for a global cyber intrusion campaign targeting intellectual property and confidential business information, including infectious disease research. Targeted industries around the world included aviation, defense, education, government, health care, biopharmaceutical and maritime.

And lastly, in July 2021, NSA, FBI, CISA publicly released more than 50 cyber tactics and tools used by Chinese state-sponsored hackers against the U.S. as well as mitigation steps for US companies.

Over the past decade we have seen CCP cyber and insider threat breaches and criminality to such a level I fear we are becoming numb when it is identified. One such event was the Equifax breach in May of 2017. As former head of U.S. Intelligence, I consider this to be one of the CCP's greatest intelligence collection successes. More than 145 million Americans had all their financial data, nicely aggregated, to the CCP along with Equifax's trade secrets on how they acquired such data. That is every American adult. Anthem lost 80 million medical records in 2015, Marriott lost 500 million guest's records in 2014, and in 2015 OPM lost 21 million records to China's cyber theft. I would be remiss if I left out China's breach of multiple cloud service providers in which China obtained access to over 150 companies' data.

The Insider Threat epidemic originating from the CCP has been nothing short of devastating to the U.S. corporate world. Anyone can go to Department of Justice's web site and search economic espionage. The result is hard to swallow. And those listed cases are just what was identified, reported by a U.S. company, and then prosecuted. I will touch on the impact of economic espionage a bit later. Just this past April 2021, a former scientist at Coca-Cola and Eastman Chemical was convicted of economic espionage & theft of trade secrets, on behalf of the CCP. The scientist stole trade secrets related to formulations for bisphenol-A-free (BPA-free) coatings for the inside of beverage cans. The scientist was working with a corporate partner inside China to monetize the stolen data utilizing the new company in China. The CCP had invested millions in the shadow new company in China. The stolen trade secrets cost US companies approximately \$120 million to develop per open-source reporting. This is one example from the dozens identified in the past five years.

When you combine the persistence of intent and capability for the CCP's cyber intrusion programs, with the onslaught of Insiders being arrested, indicted and convicted by the FBI and DOJ over the past decade, it creates a formidable mosaic of insurmountable levels. But it is not. With a comprehensive whole of government and whole of society approach of defending against China with awareness, strategy, enhanced defenses, practical mitigation programs, and a patriotic value-based return to great competition, the U.S. can begin change the course of history as I see it now.

So, what is current and next in the targeted view scope by the CCP? Look no further than President Biden's economic growth agenda and proposed congressional legislation detailing our strategic movement in the next few years. Electric vehicles, battery technology, bio agriculture, precision medicine and sustainable green energy. China manufactures, produces, and delivers 80 percent to the anti-biotics sold and utilized in the U.S. We cannot afford to continue to

allow China to control and/or manipulate our supply chain and potentially hold us hostage in the future.

I would be remiss if I did not reference the strategic and aggressive nature in which the CCP conducts malign foreign influence in the U.S. Unlike Russia's persistent attempts to undermine our democracy and sew discord, mostly at the federal level and within the U.S. Congress, the CCP strategically, and with precision, conducts nefarious influence campaigns at the state and local level.

I have referenced the influence success in Hollywood and the self-censoring which occurs to not offend China to ensure sales of their product to the Chinese markets. When it comes to Taiwan, the CCP becomes the most aggressive. Oftentimes state and local officials agree to travel to Taiwan to identify or negotiate economic investment opportunities. The CCP will undoubtedly apply holistic pressure to the local officials, from overt threats to subtle promises of economic infusion at the city or town level. There is most likely a company or business located inside an official's town which is heavily influenced or leveraged by prior investment by the CCP. China will apply pressure to that U.S. company and threaten to slow down production or manufacturing in China if the company officials do not apply their respective influence on the elected leader to not travel to Taiwan. This state or local official, or even U.S. Congressperson, may have no knowledge of China's intent beneath the surface. At the same time, and not coincidentally, an op-ed or article will appear in the local newspaper downplaying economic investment opportunities in Taiwan and championing alternative efforts in China.

#### **WHY IT ALL MATTERS:**

In 2020, the estimated economic loss from the theft of intellectual property and trade secrets, JUST from the CCP, and JUST from known and identified efforts, is estimated between \$300 Billion and \$600 Billion per year (Office of the U.S. Trade Representative). To make it more relevant to Americans reading this, it is approximately \$4,000 to \$6,000 per American family of four...after taxes.

Additionally, in 2010 China had one company in the top ten of Forbes' Global 2000 list. In 2020 they had five. That is a 500 percent increase in one decade. Competition is great and necessary and is what made America the global leader we are today. However, I would proffer China's growth through any and all means is much less than fair competition. To reiterate, competition is always good, and necessary in any aspect. My question is...are we really competing? If we do not alter how we compete on the global ecosystem with awareness of China's methodology and practices, we will not be able to sustain or global position as the world leaders in technology, manufacturing, education, science, medicine, research, development, and thoughts and ideas. We must aggressively enhance our willingness to not only understand these threats and unfair practices

but be willing to create a robust public private partnership with intelligence sharing to combat the CCP while at the same time staying true to the values, morals, and rule of laws made America the greatest country in the world.

The Senate's recent passage of a bill to bolster competition and provide the much-needed resources to do so is a great start down this long road. However, we must also protect the fruits of this legislative labor from being stolen and siphoned out of the U.S. by the same techniques China successfully utilizes today. Otherwise, we will continue to conduct research and development which the CCP will obtain, legally, and illegally, to bolster their economic, geopolitical and military goals of global dominance well into the future.

In closing, I would like to thank this committee, and the Senate writ large, for acknowledging the significant threat posed by China, not only by holding this hearing, but with all the recent legislative actions the past year on combatting this threat as well as driving enhanced competition. Continuing to combat the threat posed by the CCP will take a whole of nation approach with a mutual fund analogous long-term commitment. Such an approach must start with robust and contextual awareness campaigns. The WHY matters. Regarding these awareness campaigns, we must be specific and reach a broad audience, from every level of government to university campuses, from board rooms to business schools, educating on how China's actions impair our competitive spirit by obtaining our research and development, trade secrets and intellectual property, and degrading our ability to maintain our role as economic global leaders. I have provided some recommendations for this committee, the IC, the administration, academia, research and development, as well as CEOs and board of directors in our holistic efforts to detect and deter these threats, as well as educate, inform, and compete. Our nation needs strategic leadership now more than ever, particularly when we face such an existential threat from a capable competitor who is looking beyond competition to the global dominance.

Lastly, I would like to state for the record the significant national security threat we face from the Communist Party of China is NOT a threat posed by Chinese people, as individuals. Chinese Nationals, or any person of Chinese ethnicity here in the U.S., or around the world, are not a threat and should NOT be racially targeted in any manner whatsoever. This is an issue pertaining to a communist country, with an autocratic dictator who is committed to human rights violations and stopping at nothing to achieve his goals. As a nation, we must put the same effort into this threat as we did for the terrorism threat. The threat from China, particularly with respect to the long-term existential threat is hard to see and feel, but I would suggest it is much more dangerous to our viability as a nation.

## **Recommendations:**

The holistic, and existential threat posed by the CCP is one of the few bipartisan agreements in the US Congress today. We must take this opportunity to expeditiously advise, inform, and detail the threat to every fabric of our society, and why it matters. We must, as a nation, compete at the highest level possible while at the same time understand why we are doing so, and what is at stake.

1. Enhanced and aggressive real time and actionable threat sharing with private sector. Create an Economic Threat Intelligence entity which delivers actionable, real time threat information to CEOs, Boards of Directors, state and local economic councils to enable risk-based decision making on investments and partnerships. The analogy would be the Financial Services ISAC. This intelligence delivery mechanism should include the Intelligence Community, FBI, and CISA and have at its core constituency state and local entities at risk and utilize existing vehicles such National Governors Association and the Chamber of Commerce to increase threat awareness of illicit activities investment risk at the state and local level.
2. The Senate must ensure the Intelligence Community is leaning aggressively forward in providing collected intelligence pertaining to plans and intentions, as well as nation state activities, in software, coding, supply chain and zero-day capabilities. The U.S. Government must be more effective in providing intelligence to the private sector. Enhanced declassification of collected intelligence with respect to threats to our economic well-being, industries, and companies must be delivered at speed to impacted entities prior to the threat becoming realized.
3. Implementation of the legislatively proposed Malign Foreign Influence Center. Ensure the private sector will be a constituent of the intelligence derived.
4. Bipartisan congressionally led “China Threat Road Shows” to advise and inform of the threat to CEOs, Governors, and Boards of Directors in critical economic, research and manufacturing sectors.
5. Close governance and oversight of proposed China Competition legislation with measurable outcomes and effectiveness reviews. Particularly in the research and development space.

6. Create a panel of CEOs who can conversely advise and inform Congress, the IC, and U.S. Government entities on perspectives, challenges, and obstacles in the investment arena and private sector. Currently, there is no such venue existing. I would recommend a *Business Round Table* type of framework. Membership should be diverse and include but not limited to the following sectors: Financial Services, Telecommunications, Energy, Bio Pharmaceutical, Manufacturing, Aerospace, Transportation, Private Equity and Venture Capital. Select key government participants and encourage actionable outcomes. This entity should be co-chaired by a CEO from this group.
  
7. Create a domestic version of the State Department's Global Engagement Center. The IC, and U.S. government needs a "sales and marketing" capability which can partner with U.S. business and academia to guide new and emerging threat intelligence, answer pertinent questions, and construct awareness campaigns against the threat from the CCP and other similar issues.
  
8. Establish an over-the-horizon panel to discuss, in a public forum, emerging threats posed to the long-term economic well-being of America. The first topic should take a close look at the strategic investments the CCP is making into state and local pension plans, as well as the Federal Thrift Savings Plan.
  
9. Immediately create a Supply Chain Intelligence function which can sit both in the Intelligence Community as well as outside to facilitate real time intelligence sharing. This entity should include members of the private sector skilled in understanding our supply chain and who can expedite reacting to emerging threats. This entity will also be able to provide the U.S. Government cogent mitigation strategies and assistance with policy formulation to protect our vulnerable supply chain from persistent penetration and manipulation by China and Russia.