STATEMENT OF WILLIAM R. EVANINA
CEO, THE EVANINA GROUP

BEFORE THE HOUSE HOMELAND SECURITY COMMITTEE

AT A HEARING REGARDING "COUNTERING THREATS POSED BY THE CHINESE COMMUNIST PARTY TO THE U.S. NATIONAL SECURITY"

MARCH 5, 2025

Chairman Green, Ranking Member Thompson, and members of the Committee — it's an honor to appear before you today.

I have spent 32 years working in the U.S. Government, twenty-four of which as a Special Agent with the FBI, and as Chief of Counterespionage at the CIA.

I was tremendously honored to serve as the first Senate confirmed Director of the National Counterintelligence and Security Center (NCSC) in May 2020, leading our nation's Counterintelligence and security efforts. I served in that role since 2014.

I am here before you today as the CEO of The Evanina Group, LLC. In this role, I work closely with CEOs, Boards of Directors, and academic institutions, and senior executives of the U.S. Government to provide a strategic approach to mitigating corporate risk in a complicated global environment.

A DOMESTIC THREAT LANDSCAPE OVEVIEW

EXISTENTIAL THREAT

Our nation continues to face an array of diverse, complex, sophisticated, and unprecedented threats by nation state actors, cyber criminals, and terrorist organizations.

Unquestionably, the existential threat our nation emanates from the Communist Party of China (CCP). This comprehensive threat posed by the CCP is the most complex, pernicious, strategic, and aggressive threat our nation has ever faced. It is an existential threat to every fabric of our great nation. Now, more than ever, the private sector and academia have become the modern battlefield for which Xi's holistic efforts manifest.

Xi Jinping has one overarching goal to be the geopolitical, military, and economic leader in the world. Xi, along with China's Ministry of State Security (MSS), People's Liberation Army (PLA), and the United Front Work Department (UFWD), drive a comprehensive and whole of country approach to their efforts to invest, leverage, infiltrate, influence, and steal from every corner of the U.S. This is a generational battle for Xi and China's Communist Party (CCP), it drives their every decision.

REAL COSTS OF ECONOMIC LOSS

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 and Federal Bureau of Investigation).

To make it personal for you and your constituents, this theft equates to approximately $4,000 to $6,000 per year, per American family of four…after taxes.

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. Actually, it is said by many to be the largest theft of intellectual property in the history of the world….and it has happened just in the past decade.

Additionally, it is estimated that 80% of American adults have had all of their personal data stolen by the CCP, and the other 20 percent has had most of their personal data stolen. For Xi, the overarching vison is how to counter, compete, and push past the U.S. is goal number one.

TERRORISM REDEFINED

Congress, and the entire American democratic and capitalistic ecosystems, must first clearly understand Xi's reprehensible intentions in order to effectively mitigate the accompanying threat with our own whole-of-society approach.

We must approach this existential threat with the same sense of urgency, spending, and strategy, as we have done for the past twenty-four years in preventing terrorism in our homeland.

To set the perspective, a simple definition of terrorism is "the use of threats or violence to achieve political or ideological goals."

I would offer to this committee that we are in a terrorism event. A slow, methodical, strategic, persistent, and enduring event which requires an increased degree of urgency of both government and corporate action. It is clear that under

Xi Jinping, the CCP's economic war with the U.S. has manifested itself into a clear terrorism type of framework.

Let me be more specific. The CCP's capabilities and intent are second to none as an adversary. Cyber breaches, insider threats, surveillance and penetrations into our critical infrastructure have all been widely reported. Adding in the CCP's crippling stranglehold on so many aspects of our supply chain and the result is a montage of domestic vulnerability of unacceptable proportions.

Recent nefarious and disturbing areas of the CCP's actions include VOLT and SALT TYPHOON, surveillance balloons, technical surveillance stations in Cuba, maritime cranes, Huawei, TikTok, strategic land purchases near military and strategic locations, influence at the state and local level, etc. When overlapped, the collage begins to paint a bleak mosaic which is beyond the blinking red metaphor. It is imperative to understand that the CCP maintains civil unrest and societal chaos as a primary pillar in any nefarious cyber penetration or attack.

EVERYTHING EVERYWHERE ALL AT ONCE

I would ask this committee: Is it not terrorism when our electrical grid or a natural gas pipeline is disabled via VOLT TYPHOON in a part of the U.S., resulting in millions of households, schools, hospitals, and buildings being without heat or electricity? What about when our telecommunications infrastructure (e.g., Verizon, AT&T, and T-Mobile) being disabled on the same day due an organized cyber-attack, precipitated by SALT TYPHOON? And if our financial services sector was impacted and had to go offline, for even a few hours, it would cause significant domestic and international chaos, societal panic, and disruption.

Are these not terror type events? If these events coincidently occur as the CCP makes their inevitable move on Taiwan, will the American people, and U.S. policy makers for that matter, have the sufficient appetite to actually defend Taiwan?

The CCP has strategically planned and implemented the ability to do just this, all at once, and all across our homeland. Hence, "terror" must be redefined beyond our framework which historically includes loved ones being injured or killed from a kinetic event.

The inability or unwillingness to look behind the curtain and visualize this clear and realistic scenario is no longer an option for anyone, especially the Congress, the Administration, U.S. governmental entities, academic institutions, and especially the private sector. In fact, the proverbial curtain to look behind no longer exists. We must immediately end the process of being victims to the CCP's actions.

SALT TYPHOON

The largest telecommunications hack, in the world, occurred in 2024. It occurred here, in the U.S., by CCP backed hackers, against the top nine U.S. based telecommunications carriers and hardware providers. The size and scope of this brazen hack has not yet been determined and will take extensive time to do so. This successful hack by the CCP provided comprehensive call and text data of subscribers, geolocation of the subscribers, and ability to listen to telephone conversations as they deemed interested. Per public reporting, the intent of the breach was to obtain court ordered warrant data issued to the carriers by the U.S. Government on Chinese targets. Similar to the OPM breach, the CCP succeeded beyond their dreams and intentions. It is much worse than that, but that is for a closed session with your U.S. Government agencies.

As an intelligence and law enforcement professional, I am beyond concerned with this access for all the obvious intelligence and counterintelligence gathering aspects. Additionally, the thought that a foreign adversary and competitor can access metadata call information and listen to conversations, is beyond astonishing, and very disheartening. As members of this Committee are fully aware, for this to happen here, legally in the U.S., a FISA or Title 3 court order, signed by a U.S. Magistrate Judge or FISA Court would be required.

FENTANYL

Let us take a look at the fentanyl epidemic. Members of this Committee are very familiar with the epidemic and the numbers. But it is important to revisit and place into comparison perspective. Thankfully we have recently seen a significant reduction in deaths caused by fentanyl overdoses. However, with over 200 Americans dying of fentanyl overdose every day (107k+ in'23), China's effect is analogous to a Boeing 737 aircraft crashing, every day, and killing everyone on board. The fentanyl epidemic is delivering the same casualty rate within the U.S. as Germany and Japan delivered to American soldiers in World War II. Currently, fentanyl overdoses per day are 50% greater than the World War I Killed-in-Action per day count. Let that sink in. And as members of this committee are already aware, most of the fentanyl precursors are manufactured in China. The fentanyl epidemic starts, and ends, with the CCP.

MARITIME PORTS

Specific adversaries (Russia/China) have been historically creative in embedding intelligence collection capabilities into products which have a legitimate use in business, commerce, technology, or operating systems (see Kaspersky Labs). The CCP has taken this concept to increasingly strategic, and potentially paralyzing levels.

The new frontier, in my opinion, is the legitimate procurement by U.S. port terminals of Chinese manufactured (Shanghai Shenhua Heavy Industries Company, Limited) ZPMC crane systems.

ZPMC is a subsidiary of China Communications Construction Company (CCCC). CCCC is a prominent contractor for the Peoples Liberation Army and Navy. Members of the Committee are aware that it is currently estimated that approximately 80% of all of the ship-to-shore goods and services entering, and exiting, the U.S. are offloaded/loaded via Chinese owned ZPMC crane systems. Additionally, these same ZPMC crane systems are used by the U.S. military to commission our Naval and Coast Guard vessels at numerous strategic ports.

ZPMC cranes offer the CCP a dual use capability for intelligence collection (cameras, sensors, tracking technology, connected software) in U.S. ports servicing heavy commercial activity as well as U.S. military bases. The ZPMC crane systems provide a supply chain vulnerability of potentially paralyzing proportions. There is interconnectivity among all the ZPMC crane systems nationwide, and shared Chinese developed software and labor. ZPMC, if ordered by the CCP, can immediately shut down maritime port operations throughout the U.S. in a time of conflict or to utilize a future economic lever.

Additionally, other elements of the product transportation supply chain are also required to enter into these contracts, including data sharing agreements, and software collaboration while working at a U.S. maritime port ecosystem in order to interface with ZPMC cranes and technology.

When the ZPMC crane system threat is stacked onto the VOLT TYPHOON cyber malware penetration, the CCP will be able to systematically, and without delay, cause instant havoc in almost every aspect of American daily operations, commerce, and safety, and at the same time instill a level of societal and business panic not seen since September 1, 2001.

In my professional opinion, and from a civilian and military perspective, this might be the CCP's most strategic operational endeavor against the U.S. thus far, outdistancing Huawei. We cannot allow it to be their most successful.

INSIDER THREAT

The Insider Threat problem, originating from the CCP, has been nothing short of devastating to the U.S. corporate world, academic institutions, and research and development organizations in the past decade, plus. The Department of Justice's web site's catalog of economic espionage indictments and convictions is staggering. The result is hard to swallow and quantify. And those listed cases only represent what was identified, reported by a U.S. company, and then prosecuted.

We need to continually highlight this issue as a key facilitator for the CCP's strategic endeavors to steal intellectual property and trade secrets, especially those developed before they are classified by the U.S. Government, as well as the CCP's strategic placement for human enabled cyber operations.

Corporate America and academia must make significant efforts to identify and mitigate insider threats to their organizations seeking to steal and/or do harm. It starts with a more substantive vetting process of applicants and incorporation of an insider threat or employee wellness program. It is too costly not to. The impacts ripple far beyond the victim company.

HOW DOES THE THREAT MANIFEST?

Intelligence services, joint ventures, science and technology investments, academic collaboration, research partnerships, front companies, mergers and acquisitions, and outright theft via insiders and cyber intrusions, initiate the comprehensive and strategic framework for how China implements their strategy.

China continues to successfully utilize "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, IT professionals, and students, are shrouded in legitimate work and research. Oftentimes, the "non-traditional" collector becomes an unwitting tool for the CCP and its intelligence collection apparatus.

China's ability to holistically obtain our Intellectual Property (IP) and Trade Secrets via illegal, legal, and sophisticated hybrid methods is beyond demoralizing. Joint ventures, creative investments into our federal, state and local pension programs, collaborative academic engagements, Sister City Programs, Confucius Institutes and similar programs on university campuses, 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.

ACADEMIA A LEADING TARGET

The threat posed by China to U.S academia, as well as research institutions (including federal), is deep, pervasive, and decades long. The past decade of indictments and prosecutions have highlighted the insidiousness of China's approach to obtaining early and advanced scientific research and data.

Additionally, China has expertly learned and manipulated the complexity and shrouding of gifts and funding at U.S. colleges and universities, particularly when tied to federal grants. On-going academic partnerships by U.S. universities with CCP cultural programs (Confucius Institutes) and CCP funded research institutions is increasingly problematic, and one-sided.

For example, the University of Michigan, and other universities, recently severed ties with China's Shanghai Jiao Tong University (SJTU). SJTU has historically been tied to the CCP's intelligence and cyber hacking programs. The University of Michigan's brave and bold decision was only possible after the university was provided briefings, intelligence, and data as to the nefarious history and activities of SJTU by this Congress, and the FBI.

Universities need to be sufficiently advised of ongoing threats and risk in order to make sound risk-based decisions on said partnerships. Additionally, universities who continue to engage in these CCP partnerships with known nefarious activities need to be held accountable for such relationships.

There is a clear void in this problem set which requires immediate fixing. The U.S. Government, specifically the FBI, NSA, DHS, and others, must be forward leaning in dissemination of known threat intelligence to academia and research institutions. Such effort is critical to enable immediate and strategic risk-based mitigation decisions to protect not only ideation and trusted development of intellectual property, but also individual university brands.

This is increasingly important as we are in a high-speed technology race with China and cannot afford for China's continuance of easy theft and hence, not earning their place in this critical twenty-first century competition for technology dominance. I address this further in my recommendations.

ACADEMIC DUE DILIGENCE AND COMPLIANCE

U.S. academic and research institutes must engage in rigorous due diligence and compliance programs. I spend a considerable amount of business with academic institutions advising and informing them on due diligence and compliance efforts to identify and mitigate potential areas of concern with foreign students, professors, and researchers. Recently, an executive of a very prestigious U.S. university stated: "I assumed the Department of State vetted these students

prior to coming on campus. What do you want us to do?" This assumption, and related question, is very common and very problematic.

The U.S. possesses the greatest catalog of academic and research institutions and entities the world has ever seen. The U.S. continues to not only be the leaders in the world, but with such, we attract the best and brightest from around the world. The collaborative nature of academia is primary to its success; however, it is also its greatest vulnerability.

Vetting of foreign national students, faculty and research, if it occurs, is nascent at best, and in just a few institutions. The dilemma and complexity I hear from institutions is understandable. However, we can no longer continue to allow the CCP to obtain the ideation, hard work, research, and patent ready results, from U.S. academic and research institutions without any effort to defend such.

This situation is also similar to U.S. government entities such as the National Institute of Health, National Science Foundation, Department of Energy, National Labs, and so many others. To ensure security of our hard work and related product, compliance and due diligence must be a priority if we have any chance at slowing down the CCP from obtaining classified, and unclassified, research with minimal difficulty.

INDUSTRIES LEADING AS TARGETS

China's key priorities for obtaining U.S. based technology and know-how, pursuant to their publicly available "Made in China 25 Plan" are Aerospace, Deep Sea Technology, Biotechnology, Information Technology, Advanced Manufacturing, Clean Energy, Electric Battery Technology, and DNA/Genomics.

Any CEO or Board of Directors engaged in any of these critical industries, and within the vertical supply chain, must understand the threat posed to them and work to identify risk-based mitigation strategies. This is a zero-sum game.

"Military-Civil Fusion" is undoubtably a strategy employed by the CCP to drive Xi's movement to global technological and military dominance. However, it is too often viewed through a western based filter and related bias. In China, there is no fusion of military and civilian efforts. They are ONE, working together, and in unison. Unlike the U.S. and other western-based democratic nations, there does not exist a bifurcation between government, military, and the private sector. I would even include the education ecosystem in this mosaic. There is one China. Xi's China. Everything, and everyone, works toward a common goal in China, which is the betterment of China.

Additionally, the People's Liberation Army (PLA) and Ministry of State Security (MSS) have never been so collaboratively intertwined with respect to common goals and aggressiveness of action as they have been the past five to ten

years. If the PLA needs a specific technology for military capability to copy or reverse engineer, the MSS will acquire it through any means necessary and will employ every legal, and illegal, tool as referenced earlier, in obtaining the necessary technology.

CHINA DOES NOT PLAY BY ANY RULES

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

To further the CCP's unlevel 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. Additionally, many of the CCP's largest corporate leaders and CEO's have gone missing.

Boards of Directors and investment leaders must begin to think strategically about what the long-term threat impact the CCP presents and how their investments, decisions, and unawareness of the long-term threat impact their respective businesses and industries. This threat is woven with our national security, economic stability, and endurance of our republic. As a nation, and if we truly want to compete with China, we must move toward a more intertwined risk-based intelligence sharing effort between the U.S. government, corporate America, and academic institutions.

CHINA'S NEED TO KNOW LAWS

In 2017, the Communist Party of China issued new state laws to facilitate the perniciousness of their efforts to obtain data, from everywhere, and in any way. Three specific portions of these laws should be understood, and be an enduring reminder to CEOs, General Counsels, Chief Data Officers, CIOs, CSOs 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.

These laws carry with every Chinese citizen whether they reside in Beijing, or anywhere else in the world, regardless of their employer. Hence, a Chinese National working at a U.S. company is always at risk for answering to the CCP's data collection apparatus.

YOUR DATA IS CHINA'S DATA

As a cautionary tale, 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, without exception. This includes any third-party data as well. The analogy is a U.S.-based company entered into a business deal or partnership with a company from another country. In order to do business, the U.S. company would be required to provide all relevant and requested data from their company, as well as the partner company, to their customer agency, such as the NSA, CIA and FBI. To reiterate, the operational and legal tempo of the CCP is difficult to visualize and understand while looking through western and democratic lenses. There is no bifurcation between the CCP and corporate ecosystem. It is one China.

MALIGN INFLUENCE

Malign foreign influence has increased dramatically in the U.S. in the past decade. Russia, China, and others have been very active in this activity and with varying degrees of success. Measuring such activity has proven to be not a perfect science.

China is strategic and precise as they successfully influence at the state and local levels of the U.S. I want to briefly touch on a few key areas.

The first is economic investment. Chinese investments in key industries such as real estate, agriculture, advanced manufacturing, and technology have raised significant concerns. These partnerships often take the form of "Sister City Programs but can also be business partnerships between a city or small town and a CCP owned or controlled company. Investments in U.S. critical infrastructure at the local level is also on the rise which creates an entire separate category of concern.

The CCP takes advantage of small towns and cities increasing need for economic solicitation of funds. CCP partnerships with Economic Development professionals provides the most immediate and impactful results. The town, or city, receive immediate investment and the CCP obtains a foothold, access, or future opportunity for strategic purposes. Local Economic Development professionals have no idea of the ultimate purpose or intent of such a partnership.

Political donations and lobbying are another serious concern. The CCP's strategic approach to identify current, and future, political leaders and elected officials and invest in their future continues to be problematic. The investment can take form in direct financial support to a campaign, lobbying, or placing CCP loyalists into the inner circle of an elected official to influence decision making to benefit CCP interests or individuals supporting CCP efforts.

The most common initial step is the official invite of a newly elected federal, state, or local official for an all-expense paid trip to China with family and friends where the CCP will offer investments and inexpensive solutions to the elected official's economic challenges. As well, the CCP will gain access to the elected official's mobile devices.

The obvious and immediate need is to have a platform where state and local (and even federal) elected officials can receive substantive training and awareness of how these issues manifest in their state, city or township.

THE NEED FOR STRATEGIC LEADERSHIP

In closing, I would like to thank this Committee for acknowledging the significant threat posed by China by holding this hearing. Continuing to drive awareness, and more importantly, combat the threat posed by the CCP will take a whole-of-nation approach with a mutual fund type long-term commitment. Such an approach must start with robust and contextual awareness campaigns, like this Committee holding this hearing. The WHY matters.

Regarding these awareness campaigns, we must be specific and reach a broad audience, from state and local governments to academia, from board rooms to business schools, educating on how China's actions impair our competition by obtaining our research and development, trade secrets and intellectual property, and degrading our ability to maintain our role as economic global leaders.

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 global dominance. We have to catch up, mitigate and inflict costs on China in an expedited fashion. Doing such will entail strategic leadership leading a whole-of-society approach is imperative.

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. This is an issue pertaining to a communist country, with an autocratic dictator who is committed to human rights violations and will stop 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 as dangerous, if not more dangerous, than terrorism to our viability as a nation.

RECOMMENDATIONS:

The holistic and existential threat posed by the CCP is one of the few bipartisan areas of agreement in the U.S. Congress today. We must, as a nation, compete at the highest level possible while at the same time understand the gravity and urgency, and what is at stake.

Below are some recommendations:

1. Implement an aggressive real time and actionable threat sharing by the U.S. Government 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. This intelligence delivery mechanism should include the Intelligence Community, FBI, Department of Commerce, Department of Treasury, and CISA. The core constituency should be 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. Congress must ensure U.S. government agencies are leaning aggressively forward in providing collected intelligence to corporate America 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 expeditiously to the private sector.** Enhanced declassification of collected intelligence (especially in the technology arena) 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. **Maintain bipartisan congressionally led public hearings** to advise and inform CEOs, Governors, and Boards of Directors in critical economic, research and manufacturing sectors of the threat posed by the CCP, and how they are targeted.

4. **Create a panel of CEOs who can advise and inform Congress and U.S. Government entities on perspectives, challenges, and obstacles in the investment arena and private sector supply chain dilemmas.** I would recommend a *Business Round Table* type of framework. Membership should be diverse and include but not be limited to the following sectors: Financial Services, Telecommunications, Energy, Bio Pharmaceutical, Manufacturing, Aerospace, Transportation, Private Equity and Venture Capital. This entity should be co-chaired by a CEO from the above group.

5. **Establish an over-the-horizon panel to discuss, in a public forum, emerging technology which may potentially pose a long-term threat (AI/ML, Quantum, Aerospace) 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, CCP's strategic land purchases, Sovereign Funds, as well as foreign investment into the Federal Thrift Savings Plan and other state/local retirements vehicles.

6. **Reestablish the National Security Higher Education Advisory Board (NSHEAB).** This board should have 25 college and university Presidents as members with a Chair and Co-Chair and be housed and facilitated by the Federal Bureau of Investigation in partnership with the CIA and NSA. All members will be provided security clearances at the Top-Secret level in order to be provided real time threat and awareness information the U.S. Government possess to help guide academia in risk-based decisions and partners. This entity existed until the FBI closed the program in 2014.

7. **Create a National Training Center for elected officials.** This center will provide baseline training to newly elected officials and their staff on what malign influence looks like (examples of recent situations) and how to best mitigate such efforts. Additionally, what will surely occur on your first trip to China as an elected official, particularly with your mobile devices.

8. **Create a platform where each Governor of the U.S. can establish his/her own CIFIUS-Lite program to identify and mitigate nefarious economic investments and land purchases within their respective states.** This framework will provide intel and data sharing from the Treasury Department's CIFIUS Program, the FBI, DHS, and other law enforcement and intelligence entities to assist individual U.S. states on what to look, how such nefarious activity manifests at the local level, and how to most effectively mitigate.

   Again, I am honored to be here today and thank the Committee for holding this hearing to better understand and mitigate the existential risk posed the CCP to our national security.