STATEMENT OF WILLIAM R. EVANINA
CEO, THE EVANINA GROUP

BEFORE THE HOUSE JUDICIARY SUBCOMMITTEE ON THE COURTS, INTELLECTUAL PROPERTY AND THE INTERNET

AT A HEARING CONCERNING "INTELLECTUAL PROPERTY AND STRATEGIC COMPETION WITH CHINA: PART I"

MARCH 8, 2023

Chairman Issa, Ranking Member Johnson, and Members of the Committee — it's an honor to appear before you today. I have spent 31 years of my adulthood working the U.S. Government. Twenty-four of which were with the FBI, CIA, and as the Senate Confirmed Director of the National Counterintelligence and Security Center.

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 to provide a strategic consulting in an effort to mitigate corporate risk in a complicated global environment. This most certainly is inclusive of protecting the theft of intellectual property and trade secrets.

Getting right to the point. 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 the U.S. This is a generational battle for XI and China's (CCP) Communist Party, it drives their every decision.

This existential threat TO America begins with the comprehensive, pernicious, and strategy-based theft of U.S. Intellectual Property and Trade Secrets.

ECONOMIC SECURITY

Economic security is national security. Our economic prosperity, and security of such, drives our prosperous economy which also provides for the greatest military and national defense the world has ever seen. However, let us be clear and honest, 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 Chinese regime.

REAL COSTS

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. To make it more relevant, and personal, it equates to approximately $4,000 to $6,000 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 happened just in the past decade.

HOW CHINA STEALS INTELLECUAL PROPERTY

The threat from China pertaining to U.S. academia is additionally both wide, and disturbingly deep. Intelligence services, science & technology investments, academic collaboration, research partnerships, joint ventures, front companies, mergers and acquisitions, and outright theft via insiders and cyber intrusions, set the comprehensive and strategic framework for how China implements their grand strategy.

Additionally, we see creative investments into our federal, state and local pension programs, collaborative academic engagements, Sister-City Programs, Confucius Institutes on U.S. campuses, Talent Recruitment Programs, investments in emerging technologies, and utilization of front companies frequently manifesting the strategy into our corporate, research, and academic ecosystems. All of these strategic, and coordinated, efforts continue to be a frequent part of strategically acquiring the thoughts and ideas of our researchers, as well as development of those ideas pre and post patent application.

China also 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, and students are shrouded in legitimate work and research, and oftentimes become unwitting tools for the CCP and its intelligence apparatus.

WHAT IP DOES CHINA STEAL?

Everything. China's priorities for obtaining U.S. based intellectual property, trade secrets, ideation, and technology, pursuant to their publicly available "Made-in-China 25 Year Plan", is clear, concise, and at the same time strategic and comprehensive. Aerospace, Deep-Sea Technology, Biotechnology, Information Technology, Manufacturing, Clean Energy, Electric Battery Technology, and DNA/Genomics are just a short list of the CCP's published wish list. But any intellectual property, or trade secret, that may further China's military or civilian advancement is prime for the taking.

To illustrate the CCP's diversity of theft, prosecutions emanated from the theft of hybrid seeds (Monsanto), titanium dioxide (white paint, Dupont), glass insulation (Pittsburg Corning), and hundreds of other mind-expanding theft opportunities. In the Monsanto instance, CCP intelligence offices were captured at the airport after literally digging up the seeds in a Monsanto farm in the Midwest.

As of 2022, every itemized technology on China's "Made-In-China 2025 Plan has representation in corporate theft reporting, FBI investigations, and/or DOJ legal actions. The correlation is both stark and debilitating. The CCP puts the U.S., and the world, on notice of their requirements.

ECONOMIC WAR REQUIRES AWAARENSS AND ACTION

Any CEO, or Board of Directors, in any of these critical industries must become aware of the threat posed to them. They must work efficiently and aggressively with their security and legal apparatus, as well as outside experts, to identify risk-based mitigation strategies. This needs to occur yesterday.

The proverbial salt in the wound of intellectual property theft is when the CCP steals our thoughts, ideas, patents, and technology, and manufactures that same technology inside China, and the sells it back to American companies and around the world. One needs to look no further than the American Superconductor Corporation (AMSC) for just a glimpse of the long-term impact to economic espionage and theft of intellectual property. Additionally, one must factor in all the manufacturing plants which were not built in the U.S., 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 sells that same U.S created product and a significant reduction in real costs. The short-term pain hurts, but the long-term economic loss is debilitating.

I would like to reference just a few recent criminal cases which depict the comprehensive strategy, depth of strategy and criminality, and success of the CCP's nefarious efforts to steal our intellectual property and trade secrets.

MICRON TECHNOLOGIES

The Micron investigation meticulously lays out the structured process for China's strategy and process in illegally obtaining intellectual property and trade secrets to benefit China's military and civilian advancements. In this particular case, China knew they could not develop the technology and subsequently manufacture "chips" to compete with the U.S. Hence, they decided to illegally steal the technology from MICRON instead. To best illustrate, I have incorporated some narrative from DOJ's indictment.

According to the indictment, the defendants were engaged in a conspiracy to steal the trade secrets of Micron Technology, Inc. (Micron), a leader in the global semiconductor industry specializing in the advanced research, development, and manufacturing of memory products, including dynamic random-access memory (DRAM). DRAM is a leading-edge memory storage device used in computer electronics. Micron is the only United States-based company that manufactures DRAM. According to the indictment, Micron maintains a significant competitive advantage in this field due in large part from its intellectual property, including its trade secrets that include detailed, confidential information pertaining to the design, development, and manufacturing of advanced DRAM products.

Prior to the events described in the indictment, the PRC did not possess DRAM technology, and the Central Government and State Council of the PRC publicly identified the development of DRAM and other microelectronics technology as a national economic priority. The criminal defendants are United Microelectronics Corporation ("UMC"), a Taiwan semiconductor foundry; Fujian Jinhua Integrated Circuit, Co., Ltd. ("Jinhua'"), a state-owned enterprise of the PRC; and three Taiwan nationals: Chen Zhengkun, a.k.a. Stephen Chen, age 55; He Jianting, a.k.a. J.T. Ho, age 42; and Wang Yungming, a.k.a. Kenny Wang, age 44. UMC is a publicly listed semiconductor foundry company traded on the New York Stock Exchange; is headquartered in Taiwan; and has offices worldwide, including in Sunnyvale, California. UMC mass produces integrated-circuit logic products based on designs and technology developed and provided by its customers. Jinhua is a state-owned enterprise of the PRC, funded entirely by the Chinese government, and established in February 2016 for the sole purpose of designing, developing, and manufacturing DRAM.

According to the indictment, Chen was a General Manager and Chairman of an electronics corporation that Micron acquired in 2013. Chen then became the president of a Micron subsidiary in Taiwan, Micron Memory Taiwan ("MMT"), responsible for manufacturing at least one of Micron's DRAM chips. Chen resigned from MMT in July 2015 and began working at UMC almost immediately. While at UMC, Chen arranged a cooperation agreement between UMC and Fujian Jinhua whereby, with funding from Fujian Jinhua, UMC would transfer DRAM technology to Fujian Jinhua to mass-produce. The technology would be jointly shared by both UMC and Fujian Jinhua. Chen later became the President of Jinhua and was put in charge of its DRAM production facility.

While at UMC, Chen recruited numerous MMT employees, including Ho and Wang, to join him at UMC. Prior to leaving MMT, Ho and Wang both stole and brought to UMC several Micron trade secrets related to the design and manufacture of DRAM. Wang downloaded over 900 Micron confidential and proprietary files before he left MMT and stored them on USB external hard drives or in personal cloud storage, from where he could access the technology while working at UMC.

HUAWEI TECHNOLOGIES

The Huawei indictment, which included charging their Chief Financial Officer, WANZHOU MENG, illustrates not only the perniciousness of the CCP's efforts, but also as how high in China's civilian corporations' explicit direction is provided to stop at nothing to succeed. Later in this document I list the Chinese laws which mandate partnership, collaboration, and sharing of data between the CCP government, military, and every civilian business, without exception. Below is just a piece of DOJ's indictment illustrating the theft of intellectual property and trade secrets.

The 16-count superseding indictment also adds a charge of conspiracy to steal trade secrets stemming from the China-based company's alleged long-running practice of using fraud and deception to misappropriate sophisticated technology from U.S. counterparts.

As revealed by the government's independent investigation and review of court filings, the new charges in this case relate to the alleged decades-long efforts by Huawei, and several of its subsidiaries, both in the U.S. and in the People's Republic of China, to misappropriate intellectual property, including from six U.S. technology companies, in an effort to grow and operate Huawei's business. The misappropriated intellectual property included trade secret information and copyrighted works, such as source code and user manuals for internet routers, antenna technology and robot testing technology. Huawei, Huawei USA and Futurewei agreed to reinvest the proceeds of this alleged racketeering activity in Huawei's worldwide business, including in the United States.

The means and methods of the alleged misappropriation included entering into confidentiality agreements with the owners of the intellectual property and then violating the terms of the agreements by misappropriating the intellectual property for the defendants' own commercial use, recruiting employees of other companies and directing them to misappropriate their former employers' intellectual property, and using proxies such as professors working at research institutions to obtain and provide the technology to the defendants. As part of the scheme, Huawei allegedly launched a policy instituting a bonus program to reward employees who obtained confidential information from competitors. The policy made clear that employees who provided valuable information were to be financially rewarded.

Huawei's efforts to steal trade secrets and other sophisticated U.S. technology were successful. Through the methods of deception described above, the defendants obtained nonpublic intellectual property relating to internet router source code, cellular antenna technology and robotics. As a consequence of its campaign to steal this technology and intellectual property, Huawei was able to drastically cut its research and development costs and associated delays, giving the company a significant and unfair competitive advantage.

GENERAL ELECTRIC

General Electric (GE), founded in 1892, is one of the oldest, proudest, most recognizable brands, and influential corporations in our nation's history in both the corporate landscape, as well as in partnering with our national security apparatus.

Because of this success and history of delivering technology and capability, GE has unfortunately been a targeted victim of the nefarious efforts of the CCP in recent years. One example I wish to provide the subcommittee illustrates the strategy of the CCP to illegally obtain intellectual property and trade secrets which benefit both China's military growth and competitiveness, as well as their economic and civilian growth and competitiveness.

This past November, YANJUN XU was sentenced to twenty years in federal prison for "targeting American aviation companies, recruited employees to travel to China, and solicited their proprietary information, all on behalf of the government of the People's Republic of China (PRC)." (DOJ Press Release 11/16/2022)

XU was not the typical non-traditional collector the CCP sends to the U.S. to obtain intellectual property and trade secrets. XU is a highly trained intelligence officer. XU is a Deputy Director in China's Ministry of State Security (MSS). XU was the leader of the CCP's global effort to obtain aviation technology to benefit China's civilian and military programs. In this instance, it was GE Aviation's composite aircraft engine fan module. GE was the only company in the world to develop and possess this proprietary acoustical technology.

This particular case clearly draws a direct and bold line from President XI to the CCP's "Made in China 25" plan, to the MSS, and right to GE. Additionally, and not to be minimized, this was the first time an intelligence off er from China's MSS was indicted and convicted under the economic espionage statute. Additional and related indictments set forth XU's recruitment of other "insiders" in the U.S. to illegally obtain intellectual property and trade secrets from U.S. corporations, research institutes, and academia.

THE GE BIGGER PICTURE

As I stated in the beginning of the statement for the committee, XI has one goal, to be THE global leader. This includes civilian aviation.

Next month China will roll out the first flight of their COMAC 919 (C919) single isle passenger airliner. The C919 is a narrow-body passenger jet built by the Commercial Aircraft Corporation of China (Comac), a state-owned company based in Shanghai.

The clear intention of this effort is to both compete, and eventually overtake, both Boeing and Airbus, as the leader in global passenger transportation. China can build their aircraft quicker and cheaper, and as most of their stolen technology which eventually makes its way into the global market, is stolen technology delivered at half the market price.

As recently depicted and illustrated by CROWDSTRIKE, and other media outlets, almost the entire make-up of the C919 is stolen technology from numerous aviation and technology industries from around the world. (I have attached the graphic for the subcommittee).

NO LIMITS TO TARGETED VICTIMS

The past ten years of indictments and prosecutions have highlighted just the surface of the insidiousness of China's approach to obtaining early and advanced technologies, ideation, research, intellectual property and trade secrets.

Boards of Directors and investment leaders must not only have a comprehensive understanding of the CCP's intentions, but as well look beyond the next fiscal quarterly earnings call and 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.

CHINA CREATS UNFAIR PLAYING FIELD

In 2017, the Communist Party of China issued new state laws to facilitate the perniciousness of their efforts to obtain data, from everywhere, but a whole of Chinese society approach. 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 holding and ultimate 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 from another country 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 unleveled economic playing field, out of the 15 largest companies inside China, 13 are either owned by the CCP or run by the CCP.

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 he 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 and obtain the requisite funding to from the Federal Reserve Bank.

INSIDER THREAT

The Insider Threat epidemic originating from the CCP has been nothing short of devastating to the U.S. corporate world and their success in obtaining intellectual property. Go to Department of Justice's web site and search economic espionage. The result is hard to contemplate and will surely provide a disbelieving cognitive pause. And those listed cases are just what was identified, reported by a U.S. company, and then prosecuted.

In one particular example, in 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 of the CCP's cyber intrusion programs, with the onslaught of insiders being arrested, indicted and convicted by the FBI/DOJ over the past decade, it creates a formidable mosaic of intellectual property theft at seemingly insurmountable levels.

So, what is current and next in the targeted areas of 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. Look at every grain of it. Electric vehicles, battery technology, bio agriculture, precision medicine and sustainable green energy.

WHY IT ALL MATTERS

In closing, I would like to thank this subcommittee, and the Judiciary Committee, for acknowledging the significant threat posed by China, not only by holding this hearing. 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 and economic 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 areas of concern in the US Congress today. Congress must take this opportunity 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. The CCP delivers their Five-Year Plans, which are public, and clearly designate the technologies they require, and hence, becomes a framework for their comprehensive theft machine. Add to this plan, the clandestine collection by our Intelligence Community designating their modes operandi and provide this framework directly to targeted industries. Create an Economic Threat Intelligence entity which delivers this 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 is 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. Close governance and oversight of proposed China Competition legislation with measurable outcomes and effectiveness reviews to ensure the CCP is not already in the process of stealing congressionally funded research and technology.

3. 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 form this group.

4. 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.

5. 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, and the U.S investment into green energy.

6. Create a bipartisan commission to evaluate the efficacy and effectiveness of the current U.S. Paten process to create modernization and baseline security to prevent our adversaries from stealing the technology during the long patten process.