STATEMENT OF WILLIAM R. EVANINA
CEO, THE EVANINA GROUP

BEFORE THE HOUSE OVERSIGHT SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY AND GOVERNMENT INNOVATION

AT A HEARING CONCERNING "COUNTERING THE CYBERTHREAT FROM CHINA"

MAY 15, 2024

Chairwoman Mace, Ranking Member Connolly, and Members of the Sub Committee— it's an honor to appear before you today. I have spent 32 years of my adulthood working in the U.S. Government, twenty-four of which were with the FBI, CIA, and the National Counterintelligence and Security Center (NCSC).

I was tremendously honored to be the first Senate Confirmed Director of the NCSC in May of 2020 after serving 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 to provide a strategic approach to mitigating corporate risk in a complicated global environment.

THE CHINA 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 confronts is from the Communist Party of China (CCP). The 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.

ONE GOAL

Getting right to the point, 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 (UFED), 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. The U.S private sector, academia, research and development entities, and our core fabric of ideation, has become the geopolitical battlespace for China.

REAL COSTS

In 2022, the estimated economic loss from the theft of intellectual property and trade secrets, JUST from the CCP, and JUST from known and identified efforts, was estimated between $300 Billion and $600 Billion per year (Office of the U.S. Trade Representative and Federal Bureau of Investigation). 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.

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 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 Xi and the CCP.

UNDERSTANDING THE CHINA THREAT

We must first clearly understand Xi's intentions and aggressively mitigate the accompanying threat with a whole-of-society approach. We must also approach this existential threat with the same sense of urgency, spending, and strategy, as we have done for the past two decades in preventing terrorism.

I would offer to this committee that we ARE in a terrorism event. A slow, methodical, strategic, persistent, and enduring event which requires a degree of urgency of government and corporate action. It is clear that under Xi Jinping, the CCP's economic war with the U.S. is manifested itself into a terrorism 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 and we have become numb to these episodes, as a nation. Add in the CCP's crippling stranglehold so many aspects of our supply chain and what results is an imbalance and domestic vulnerability of unacceptable proportions. When we move to new areas of the CCP's actions to include surveillance balloons, technical surveillance stations in Cuba, maritime cranes, Huawei, TikTok, strategic land purchases, foreign influence, etc., the collage begins to paint a bleak mosaic.

A NEW TERRORISM

I would ask the subcommittee is it not terrorism when a hospital, high school, police department, college, county services, or water treatment facility are shut down by a cyber-attack, breach, or ransomware event? How about a natural gas pipeline that is shut off via a malware deployment or virus? How about our electrical grid or natural gas being shut off in the winter in the northeast part of the U.S. resulting in millions of households, and buildings, without heat? How about our telecommunications infrastructure going down one day because Verizon and AT&T are hit with a cyber-attack on the same day? Lastly, what if our financial services sector had to go offline, for even a few hours, causing significant international chaos and disruption. Are these not terror events? Hence, "terror" must be redefined beyond our framework which includes loved ones being injured or dying from a kinetic event. Cyber must be an accepted portion of the lexicon we use to describe an "attack" or a "terror" event. I address VOLT TYPHOON later in this statement.

It is easy to parlay all the "would be" and "could be" scenarios as fear-based paranoia. However, intelligence and law enforcement professionals, cyber professionals and international organizations monitoring the CCP have all seen the facts regarding the nefarious intent, capabilities, and successfully deployment by the CCP.

The inability or unwillingness to look behind the curtain and visualize this existential threat is no longer an option for anyone, especially the Congress, the Administration, U.S. governmental entities, academic institutions, and the private sector. There is no more curtain to look behind.

CYBER CAPABILITIES

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

In the past year there have been reports of U.S. Cabinet officials, senior executives, and various agencies being hacked by the CCP. In my experience, this event will expand, and the number of victims will increase dramatically.

The FBI recently 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.

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.

VOLT TPHPOON

Most recently and I believe most importantly, and as this Sub Committee is aware, VOLT TYPHOON was recently discovered and disclosed by law enforcement, cyber and intelligence community entities. VOLT TYPHOON, a CCP state sponsored cyber actor, whose malware is hiding in plain sight throughout our nation's critical infrastructure. VOLT TYPHOON is not a cyber espionage activity. The primary tactics, techniques, and procedures (TTPs) is "living off the land", which utilizes already existing network administration tools to serve as proxies on respective systems. Additionally, this TTP provides VOLT TYPHOON the ability to evade detection due to its ability to blend in with normal operating systems. In my opinion, VOLT TYPHOON was deployed by the CCP for the future disruption and potentially destruction of U.S. critical infrastructure when, and if China felt necessary for military or other proposes.

Recently, in hearings held by both the House and Senate, the Directors of the FBI, NSA, and CISA provided scary details of China's VOLT TYPHOON deployment and other CCP cyber efforts within the U.S. infrastructure and ecosystem. I believe there is unfortunately more to be disclosed regarding VOLT TYPHOON's access with potentially catastrophic consequences. I believe VOLT TYPHOON is the type of state sponsored activity that can be classified in the lexicon of terror activity. Ore-operational reconnaissance and network exploitation are not tools utilized to commit espionage or steal intellectual property.

In reality, this discovery is just the latest in a long list of such penetrations I have witnessed within the past decade from the CCP, their intelligence services, as well as their protected and shielded criminal proxies. Combine this with other

known and unknown malicious malware deployed by the CCP of the past decade, which is potentially in dormant stage, or surveillance posture, and the "blinking red" mosaic issued in 2017 Annual Threat Assessment has turned to purple in our critical infrastructure.

Over the past decade we have seen CCP cyber and insider threat breaches and criminality have risen 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 a former head of U.S. Counterintelligence, I consider this, along with the OPB breach of 2015, 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. That is every adult in America. Stolen along with all the personal data was Equifax's business process and trade secrets on how they acquire and share such data from financial institutions, data brokers, and credit bureaus.

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 (via cyber actor APT10) in which China obtained access to over 150 companies' data.

HOW DOES THE CCP THREAT MANIFEST?

Intelligence services, science and 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 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.

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 U.S academia is both wide and deep. The past

six years of indictments and prosecutions have 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.

MARITIME PORTS

Specific adversaries (Russia/China) have always been creative in embedding intelligence capabilities into products which have a legitimate use in business, commerce, technology, or operating systems (see Kaspersky). 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 and accompanying technology of Chinese manufactured (Shanghai Shenhua Heavy Industries Company, Limited) ZPMC cranes. It is currently estimated approximately 80% of all of the goods and services entering, and exiting, the U.S. are offloaded/loaded via ZPMC cranes. Additionally, the ZPMC cranes are used by the U.S. military to commission our Naval and Coast Guard vessels at strategic ports. Are ZPMC cranes dual use capable for intelligence collection (cameras, sensors, tracking technology) in U.S. ports servicing heaving commercial activity and U.S. military bases? Do they provide a supply chain vulnerability due to the interconnectivity among all the ZPMC crane systems nationwide and shared Chinese developed software and labor? Can ZPMC, if ordered by the CCP, shut down maritime port operations throughout the US in a time of conflict or to utilize a future economic lever? Is VOLT TYPHOON deployed withing the ZPMC and maritime port infrastructure? Additionally, what other elements of product transportation supply chain are required to enter into contracts, data sharing agreements, and software collaboration while working at a US maritime port in order to interface with ZPMC cranes and technology? From a civilian and military perspective, this might be the CCP's most strategic endeavor thus far, outdistancing Huawei.

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. One only needs to visit the 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 just 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.

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, Artificial Intelligence, 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 with their security team and outside experts 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 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 democratic nations, there does not exist a bifurcation between government, military, and the private sector. I would even include education in this mosaic. There is one China. Xi's China. Everything, and everyone, works toward a common goal in 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 (discussed later in this statement). The MSS will employ every legal and illegal tool, as referenced earlier, in obtain necessary technology.

LONG TERM CONSEQUENCES OF TECHNOLOGY THEFT

The proverbial salt in the wound of the China's nefarious activity is when the CCP steals our ideas, patents, IP, and technology, and manufactures that same technology in China, and the sells it back to American companies and 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. However, the number of examples is numerous.

When evaluating the real impact, we must factor in all the manufacturing plants which are 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.

Currently prescient is the passage of the CHIPS and Science Act, as well as the Inflation Reduction Act. Rest assured, China has already begun their strategic, and comprehensive, efforts to acquire (both legally and illegally) any and all ideation, research, and trade secrets emanating from the extensive funding provisions and technological incentives, provided by these legislative actions.

I would offer emerging renewable energy technologies, AI technologies, and semiconductor production will be targeted most aggressively. Congress must lead and hold everyone accountable for securing our most precious technologies subsequent to these, and other efforts. Ten years from now Congress cannot be holding hearings and asking how China stole our technology, and capabilities, and are selling them back to us…. as consumers.

CORPORATE AWARENESS OF DETAILS

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, without question. 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.

WHY IT ALL MATTERS

Competition is always good. The U.S. can, and will compete with anyone, and will win. Competition is 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. Additionally, we must urgently decide that breaking the stranglehold of the CCP on our vast supply chain must end (Ford). The U.S. must engage in an aggressive and urgent redundancy effort and begin to have alternate servicing of goods, products, and technologies. Additionally, and in a parallel tract, the U.S. must develop a strategic approach to consequences for the CCP's nefarious actions. There is little deterrence for the CCP to dissuade them from continuing their nefarious, destructive, and illegal activities.

CLOSING: THE NEED FOR STRATEGIC LEADERSHIP

In closing, I would like to thank this Committee for acknowledging the significant threat posed by China, not only by holding this hearing, among many others. 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 analogous long-term commitment. Such an approach must start with robust and contextual awareness campaigns, like this Committee is successfully endeavoring. 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. 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 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 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, than terrorism to our viability as a nation.