STATEMENT OF WILLIAM R. EVANINA
CEO, THE EVANINA GROUP

BEFORE THE HOUSE SELECT COMMITTEE ON THE CHINESE COMMUNIST PARTY

AT A HEARING REGARDING "COMMANDING HEIGHTS: ENSURING U.S. LEADERSHIP IN THE CRITICAL AND EMERGING TECHNOLOGIES OF THE 21ST CENTURY."

JULY 26, 2023

Chairman Gallagher, Ranking Member Krishnamoorthi, and Members of the 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.

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 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, 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.

I would ask the committee is it not terrorism when a hospital, high school, police department, college, county services, or water treatment facility are shut down by a cyber breach or ransomware event? How about a natural gas pipeline that is shut off via a malware 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? Or, our financial services sector having to go offline, for even a few hours, would cause 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.

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 intent, and capabilities, deployed 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.

HOW DOES THE 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? 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.

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 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.

EXAMPLES OF MILITARY AND CIVIL FUSION

I would like to reference just a few recent criminal cases which depict the comprehensive strategy, intent, criminality, and success of the CCP's nefarious efforts to steal our technology, intellectual property, and trade secrets for utilization in both military and civilian ecosystems.

I proffer to this committee that for every instance of technology or IP theft, there is a direct nexus to a military application, oftentimes not disclosed by the U.S. court filings, due to its sensitivity and being classified status.

MICRON TECHNOLOGIES

The Micron investigation and subsequent indictments (2019/2020) 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. Subsequent to the passage of the Chips and Science Act, the urgent race for

semiconductor technology production, and the recent hostile comments and actions of the CCP toward Micron, this investigation is even more relevant today. 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 (2019/2020), which included charging their Chief Financial Officer, Wanzhou Meng, illustrates not only the perniciousness of the CCP's efforts, but also the explicit direction provided by corporate senior leadership in China's civilian ecosystems 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.

As we continue to strive to advance 5G technology, efficiency and security, the Huawei "issue" still exists throughout our domestic landscape.

GENERAL ELECTRIC

Probably the clearest depiction of CCP strategic theft to benefit both military and civilian capabilities is the recent General Electric (GE) criminal investigation (2018). General Electric, founded in 1892, is one of the nation's oldest, proudest, most recognizable brands and influential corporations in our nation's history. GE has a been a bedrock both in the corporate landscape as well as in partnering with our national security apparatus.

Due to GE's success and history of delivering technology and capability, GE has unfortunately been consistently a target of the nefarious efforts of the CCP in recent years. One example I wish to provide the committee illustrates the strategy of the CCP to illegally obtain technology, intellectual property and trade secrets

which benefit both China's military growth and competitiveness, as well as their economic and civilian growth and competitiveness.

In November 2022, 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 was 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 PLA requirements and straight to the MSS, and right to GE. Additionally, and not to be minimized, this was the first time an intelligence officer 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 second half of the story, and the CCP's intent in this case, has military implications, and is classified.

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 and military aviation.

In May 2023, China rolled 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).

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, 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.

THE NEW NOW

What is the now in the targeted view scope by the intelligence services of the Chinese Communist Party (CCP)? Look no further than President Biden's economic and green energy growth agenda, as well as passed and proposed congressional legislation detailing our strategic economic movements in the next few years.

Electric vehicles, battery technology, bio agriculture, precision medicine and sustainable green energy are each a prime target for supply chain penetration, and IP theft, by the CCP.

The Chips and Science Act was a monumental step forward in the required partnership between the government and private sector innovation and

manufacturing. Make no mistake, our adversaries, particularly the CCP, are trying day and night to penetrate the supply chain of all the efforts involved.

FORD MOTOR COMPANY

Additionally, corporate American must be more effective and efficient at protecting and securing a sustainable supply chain for the future and thinking beyond their own earnings and incorporating a variable of national interests into their global business decision making. In just one example, this past spring, Ford Motor Company made a conscious decision pursuant to the electric vehicle proliferation to partner with Chinese company Contemporary Amperex Technology Company Limited (CATL). In my opinion, this partnership is not only selfish and misguided, but also naive to the national security and national interests of the U.S. This partnership also creates disincentives for potential investors and manufacturers who wish to develop battery technology and plants here in the U.S. Additionally, and more importantly, this partnership creates a critical supply chain dependency not only to the Chinese state sponsored CATL, but as well the CCP as a whole. An entire segment of U.S. based auto manufacturing is now potentially at risk for a future supply chain slow down, or stoppage, as leveraged by the CCP leadership for economic, or other, purposes.

The intersection of capitalism, national security, and national interests has never been clearer than in today's global economy and interconnected ecosystems.

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 week 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.

Just one month ago, law enforcement, cyber and intelligence community entities issued a joint warning regarding VOLT TYPHOON, a CCP state sponsored cyber actor whose malware is hiding in plain sight in our nation's critical infrastructure. 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. This discovery is just the latest in a long list of such penetrations the past decade. Combine this with malicious malware deployed by

the CCP of the past decade which is potentially in dormant stage, or surveillance posture, and the "blinking red" mosaic has turned to purple in our critical infrastructure.

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.

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 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 American adult. 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.

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.

CHINA DOES NOT PLAY BY ANY RULES

China plays only 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 CCP'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. 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.

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.

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.

PROTECT WHAT IS DEVELOPED

Congress' legislation of the Chips and Science Act bolsters competition and provides 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.

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.

RECOMMENDATIONS:

The holistic and existential threat posed by the CCP is one of the few bipartisan agreements 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. 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, Department of Commerce, 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 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 "China Threat Road Shows" to advise and inform CEOs, Governors, and Boards of Directors in critical economic, research and manufacturing sectors of the threat.

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) 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, as well as foreign investment into the Federal Thrift Savings Plan and other retirements vehicles.