STATEMENT OF WILLIAM R. EVANINA
CEO, THE EVANINA GROUP

BEFORE THE SENATE SELECT COMMITTEE ON INTELLIGECE

AT A HEARING CONCERNING THE COMPREHENSIVE COUNTERINTELLIGENCE THREAT TO AMERICA'S CORPORATIONS AND ACADEMIC INSTITUTIONS

SEPTEMBER 21, 2022

Chairman Warner, Vice Chairman Rubio, and Members of the Committee — it's an honor to appear before you today. I have been honored to brief this Committee on a regular basis over the past decade as the Director of the National Counterintelligence and Security Center, and as a senior counterintelligence executive in the CIA, and FBI. I was tremendously honored to be the first Senate Confirmed Director of NCSC in May of 2020. I am here before you today as the CEO of The Evanina Group, LLC. In this role, I work closely with CEOs, Boards of Directors, and academic institutions providing a strategic approach to identifying threats, vulnerabilities, and mitigating risk in a complicated global environment.

I have spent 32 years of my adulthood working the U.S. Government. Twenty-four of which with the FBI, CIA, and NCSC. For the past decade plus I have had the honor to brief this committee on counterintelligence threats, vulnerabilities, and significant issues of national security. I thank each member for your continued commitment to the Intelligence Community, law enforcement, and to the dedicated women and men around the globe defending our nation and our freedom.

THE CHANGING LANDSCAPE AND UNPRECENTED THREAT

America faces an unprecedented sophistication and persistence of threats by nation state actors, cyber criminals, hacktivists and terrorist organizations. Corporate America and academia have become the new counterintelligence battlespace for our nation state adversaries, especially the Communist Party of China (CCP).

The Communist Party of China utilizes a whole of nation approach against the U.S., and around the globe. The CCP also employs, at pace and persistence, their intelligence services (MSS/PLA) along with the strategic and programmatic efforts of science & technology investments, academic collaboration, research partnerships, joint ventures, front companies, mergers and acquisitions, and outright theft via insiders and cyber intrusions.

The CCP also continues to utilize "non-traditional" collectors to conduct the 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, researchers, and students are shrouded in legitimate work and research. The non-traditional collector can also become unwitting tools for the CCP and its intelligence apparatus while innocently participating in business or academia in America.

I proffer to this committee that we, as a government and as a nation, are not effectively and efficiently postured to combat this modern counterintelligence threat.

NON-LETAHL TERRORISM

Ten days ago, we solemnly remembered the horrific day of September 11, 2001. I spent a healthy portion of my FBI career investigating terrorism related matters, as well as being part of the Flight 93 and Anthrax investigations.

I submit to this committee we are currently in the midst of a different kind of terror attack. A strategic and systematic attack which is not kinetic or kills scores of people resulting in countless funerals and memorial services. An attack which does not occur on one day, or over a few weeks, but yet is slow and methodical, and is pernicious and destructive to the very foundation of our democracy and capitalism-based ecosystem.

The past decade has provided us a very clear mosaic of the modernization of nation state threat actors conducting persistent, strategic, targeted and sometimes destructive, cyber-attacks on American governmental institutions, U.S companies and academic institutions, and their systems, their data, and their employees. Nation states have been responsible for most of these illegal acts. As much as they are also cyber in origin, cyber is a modality utilized by nation state intelligence services. Hence, I believe, they become counterintelligence issues, with only the modality of cyber being new to the arena of an old business practice.

China, Russia, Iran, North Korea all have had their moments in the sun as aggressors, destructors, and thieves, some more than others, and some more persistent and enduring than the others. From Sony to OPM, from Anthem to Marriott, from the Department of State to the White House, from Equifax to

Microsoft, from MIT to Harvard, and from SolarWinds to Colonial Pipeline and JBL and to the scores of insiders arrested, and convicted, for working on behalf of our adversaries. There are hundreds more to list, but the mosaic is depressing, blurry, and in dire need to be addressed.

All of the cyber related breaches, data exfiltration, and in the destructive case of Sony, get attributed, with little repercussions, to the nation state with dirty hands and origins. Adding the incredible proliferation of Ransomware to the constant drum beat of cyber breaches, our critical infrastructure has never been at a more significant risk than it is today. We are at a vulnerable and precarious point in our nation's history, and future. Russia continues to actively support criminal groups inside its boarder in the Ransomware proliferation. We do make incremental steps to protect infrastructure from yesterday's technology vulnerabilities and known malware. The Intelligence Community (IC) and Department of Defense (DOD) and partnering with the FBI continue to maximize efforts to fight this fight overseas in an offensive manner. It is not enough.

It is a fact 85% of our nation's critical infrastructure is owned and operated by the private sector. The primary threat they face every day is from nation state actors. There continues to be little incentive for the private sector to significantly increase allocation of security-based resources (cyber, insider threat, or other) to provided substantiative and modern protective measures within individual companies, industries, and sectors. And at the same time, the former CEO of Equifax stated his frustration in having to defend Equifax against nation state intelligence services without the help of the U.S. Government.

Ransomware has become a terror event on its own. I would offer it is a form of terrorism when a hospital, high school, police department, college, county services, or water treatment facility are shut down for a ransomware payment? How about a natural gas pipeline I referenced earlier? How about our electrical grid, or natural gas, being shut off in January 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 ransomware on the same day? Or, our financial services sector having to go offline, for even a few hours, would cause international chaos and disruption. Are these not terror events perpetrated by, or with the support and/or protection of, nation state threat actors? I would proffer with the ensuing panic from these events beyond the infrastructure damage would be frightening. One needs to look recently at the panic resulting from the Colonial Pipeline incident. Again, "terror" must also be redefined beyond loved ones dying and attending funeral and memorial services.

The difference between now and prior to September 11, 2001, is we clearly and unequivocally see and watch the terror occurring every day. We feel it. The private sector deals with it daily. It is costing trillions of dollars. We obtain the plans and intentions of nation state leaders every day, we watch as zero days are promulgated and software is manipulated, we understand the current and future possibilities of state actors and their cyber capabilities, as well as their intent. We can and must use our collection and knowledge to protect our critical infrastructure on a more efficient and effective basis. We are not effectively doing such.

To address the rhetorical questions and supposition that we are in a different type of, terror attack, the metaphor here is basic. Currently, with respect to counterintelligence and cyber, we are watching as letters are made, placed in envelopes, sealed and then watch as they are getting placed into a blue postal box. We sometimes even know the addressee. This is a different type of terror, but terror, nonetheless. Nation-state terror. We must see it as such and treat it as such, with a sense of urgency. Our nation's sustainably and existential well-being require such.

CHIPS AND INFLATION REDUCTION ACTS VULNERABILITY

This has never been more important than with the passage of the CHIPS and Science Act. Rest assured, China, and to some extent other intelligence services, have already begun their strategic and comprehensive efforts to acquire (legally and illegally) any and all ideation, data, research and trade secrets emanating from the new funding and technological incentives, especially semiconductors. This will include China's attempt to obfuscate their intended collection of available funding in this effort though their well-established joint ventures and business partnerships.

As corporate America works towards the onshoring of critical supply chains, how do we, in parallel, ensure such efforts are not done in vain? Through renewable and natural gas technologies the United States has secured a relatively safe energy outlook compared to that of our allies whose citizens suffer from the geopolitical desires on an aggressive Russia. As the tailwinds to these energy technologies continue to grow so must our effort to protect in them. A secure national grid is the bedrock to our advanced economy, and we cannot afford for a Chinese adversary to view it as a vulnerability.

The recently passed Inflation Reduction Act secures continued natural gas exploration and an acceleration to green technologies that still must be proven in today's free market. It is incumbent upon us to protect the deployment of these technologies to secure a dependable and diversified national grid which provides American consumers with the most affordable power as possible. I cannot

underscore enough the competitive advantage our grid provides us today and we must continue the hard work to preserve this advantage and not allow our adversaries to denigrate or steal this advantage.

Ten years from now Congress cannot be holding hearings and asking how China stole all our organic ideas and capabilities and are selling them back to us. We have been victimized in this game already and must learn from the game. We have to plan for security our ideation, development and technology now, at the very beginning. All of the CCP's efforts are driven with their intent to drive their own military and civilian growth in a zero-sum game.

A MODERN VIEW AND NEED OF URGENCY

With all of the above cyber and ransomware threats, combined with the consistent, if not growing, insider threat epidemic facing our nation, it is time to take a modern view of Counterintelligence. Counterintelligence is not just catching spies from adversarial countries. Counterintelligence is not just "espionage" and "counterespionage." Granted, catching foreign spies on our soil, and around the globe, is still an important role for the intelligence and law enforcement entitles to carry out. However, counterespionage it is just a small portion of "countering" the intelligence collection efforts from our adversaries.

Numerous foreign intelligence officers continue to collect intelligence and attempt to recruit U.S. citizens to benefit their home countries. They primarily work in the out of their respective embassy complex. However, the more impactful, and costing threat, to our nation is asymmetric, via nontraditional collectors and cyber capabilities, and requires significant a radical strategic shifting of our nation's strategy, resources and commitment to defend, deter, and defeat this threat.

The lexicon of Counterintelligence has also dramatically expanded in the past decade with the development of the private sector as the new battlespace for this neo aggressive and nefarious behavior by Russia and China and their intelligence services. The impact, just from an economic espionage perspective, is that the U.S. economy loses between $400 billion and $600 billion dollars per year from theft of trade secrets and intellectual property, just from the CCP. This equates to approximately $4,000 to $6,000 per year for each American family of four, after taxes. This does not consider the economic damage, as well as damage to brand, due to cyber breaches and data exfiltration to U.S. companies, research institutions, and universities.

Additional counterintelligence lexicon manifestation includes Chinese companies such as Huawei, ZTE, and others conduct legitimate business in the U.S. and also serving as intelligence collection platforms throughout our

telecommunications networks. The new frontier may be the legitimate, and financially advantageous, procurement by U.S. port terminals and authorities of Chinese manufactured (Shanghai Shenhua Heavy Industries Company, Limited) ZPMC cranes. Are these cranes dual use capable for intelligence collection in U.S. ports servicing U.S. military bases? Do they provide a supply chain vulnerability due to the interconnectivity among all the cranes nationwide and shared Chinese developed software and labor? Who is ultimately responsible for identifying the potential counterintelligence threat prior to such a threat becoming evident when it is too late (see Huawei and Kaspersky)? The FBI, NCSC, NSA, CIA, CISA? How about CFIUS? Should CFIUS be more prescriptive and be provided enhanced authorities and responsibilities? So much of what CFIUS does is in reality, a counterintelligence issues regarding foreign investment in the U.S. by entities owned or controlled by nation states. These are some of the critical questions we must now consider with the modernization, and sense of urgency, required to rethink counterintelligence.

REIMAGINATION OF COUNTERINTELLIGENCE

It is time that we, as a government, law enforcement, Intelligence Community, Congress, and our entire nation, look at the current threat we face from nation state threat actors and cyber criminals, and treat them with the same sense of urgency, spending, and strategy we have done for preventing terrorism the past two decades. I would offer to this committee that we ARE in a terrorism event. A long, slow, methodical, strategic, persistent, pernicious and enduring event which I believe we have become numb to. We must address this terror with vigor, aggressiveness and a true public private partnership. We cannot wait for the ultimate crisis to occur, our "counterintelligence cyber 9-11", whatever that looks like.

This effort begins with an honest reimagination of what "Counterintelligence" should look like in today's complicated ecosystem. Counterintelligence is not just spies catching spies. It is for sure that, and more aggressively the recruitment of scientists, engineers, and businessmen across all aspects of American corporate, R&D, and academia. Overarchingly, counterintelligence is "countering" the intelligence collection of our adversaries. Contextually, "intelligence" in this protective mindset includes corporate data and trade secrets, academic and research ideation, research and development, and all things in the middle.

The U.S. Government is not currently postured effectively to lead the defense of our nation from nation states, their intelligence services and proxy criminal organizations. Additionally, corporate America, research institutions, and

academia must share in the burden of protecting what they ideate, develop, manufacture and then sell on the global marketplace. U.S. Government intelligence, DOD, and intelligence agencies have been extremely slow, at best, to reprogram existing resources from terrorism to nation state threats. across law enforcement, the Intelligence Community, and the Department of Defense. New, and much needed specialized resources have also not been added to this effort by the U.S. Congress with prescription of utilization.

U.S. corporations, research institutions, non-Title-50 entities, and academia must share the burned of protecting their proprietary data, trade secrets, and fundamental research. This is especially true when such organizations receive federal grants or funding. There must be a viable partnership to ensure compliance and governance of the funding and research.

NON-TITLE 50 VULNERABILITY AND URGENCY

Our nation's non-Title 50 agencies and departments have little, if any, counterintelligence professionals, tools, capabilities, resources, or authorities to protect their employees, systems, research and data from modern counterintelligence threats. Non-Title 50 agencies have seen a decade of penetration and nation state activity in their agencies and campus. From Health and Human Services' National Institute of Health, Food Drug Administration, and Center for Disease Control, to the National Science Foundation and the Department of Energy, fundamental research and emerging technologies are most at risk and continue to be persistent targets of our adversaries.

Similar to academic and corporate research and development, the collaborate nature of fundamental research provides unlimited access for our adversaries with little to no awareness and self-protection. Additionally, the CCP's successful utilization of Talent Recruitment Programs provides an unlimited supply of researchers, scientists, and engineers who study and work in the U.S. and return home to China to serve China's military and economic endeavors. This is one of the most vulnerable aspects of the fundamental research collaboration bedrock for which academia and research laboratories operate.

In this area of vulnerabilities of espionage and technology transfers, the Department of Energy, due to their span of critical research including advanced dual use technologies and nuclear weapons, might be the single most critical department/agency at risk.

When the FBI becomes involved with these non-Title 50 agencies, an opens an investigation, the damage is already done. The data our adversaries were seeking has left our shores to benefit our adversaries militarily and commercially. The subsequent investigation is just that.

OUTREACH IS CRITICAL

Until approximately a decade ago, the FBI was the primary U.S. Government outreach program to corporate America and academia. It was robust and comprehensive. There were two major portions of this effort which stood head at the forefront of these outreach efforts. The first was the National Security Business Alliance Council (NSBAC). The second was the National Security Higher Education Advisory Board. The FBI eliminated both of these efforts circa 2012. Both of these efforts require reinstatement, funding, and governance by either the FBI or NCSC, or a combination thereof to enhance threat awareness and mitigation partnership with the private sector and academia.

NCSC has filled some of this outreach void the past seven years considering the limited resources assigned to do such.

CISA has played a vital role in outreach as well in the hectic and critical cyber arena. As this committee is fully aware, a predominance of the cyber threats, warnings, and eventual attacks come from, or with the support of, intelligence services of our main nation state adversaries.

To get left of nation state threats, the first line of effort is identifying the treat, educating how it is manifested, and providing threat and warning. The current private sector and academic battlespace requires enhanced and aggressive efforts in this area. This effort, as I stated previously, entails the aggressive outreach, and sometimes declassification, of and related to the collected intelligence in the IC, DOD, and law enforcement communities. Enhanced outreach efforts will better inform CEOs, CISOs, CIOs and CSOs across our critical infrastructure landscape in real time. I would proffer that our higher education system, specifically post graduate level S&T, and R&D, should be designated a national security critical infrastructure and treated as a national security ecosystem.

NCSC, CISA, FBI, and others, provide ad-hock efforts are all in this arena, with limited resources, and variable successes. We must increase and enhance these efforts.

THE NEW LANDSCAPE

As I have previously discussed, the complexity of today's counterintelligence threat landscape in America grows exponentially every day with new and sophisticated tools, techniques, and surface areas of attack for our adversaries. Let me take a brief moment to refresh the current pillars of the 2020 Counterintelligence Strategy of America:

1. Protect the Nation's Critical Infrastructure
2. Reduce Threats to the U.S. Supply Chains
3. Counter the exploitation of the U.S. Economy
4. Defend American Democracy Against Foreign Influence
5. Counter Foreign Intelligence Cyber and Technical Operations

When Congress enacted the Counterintelligence Enhancement Act in 2002, as well as with Presidential Executive Order 12333 signed in 1981, none of the above pillars were obviously a counterintelligence concern, or even part of the deliberative process, when being crafted. Additionally, nor was the concept, and success, of the non-traditional nation state intelligence collectors and cyber operations attacking, influencing and penetrating those pillars.

The overarching threat to our nation's critical infrastructure, the protection of our supply chain, malign foreign influence, and cyber and technical operations all, with few exceptions, emanate from our nation state adversaries and/or rogue criminal entities supported by those same intelligence services. Yet, we do not classify all of these threats in the "countering intelligence" category. No specific federal entity has authority, jurisdiction, or strategic planning on these areas of threat manifested every day in our nation. We mush correct this if we are to effectively solve this problem

EXISTENTIAL CHINA THREAT

Russia poses an increased, and significant intelligence and cyber threat to the US, in both the public, and private sectors. Vladimir Putin, with his aggressive intelligence services along with loyal, highly resourced oligarchs, continue to push boundaries in numerous geopolitical and cyber arenas. Putin's goal to destabilize the U.S. and degrade our Democracy in evident every day, especially in illicit cyber activity and extensive social media malign influence campaigns. Russia will continue to conduct influence operations on our soil and toil in all of our national elections. Subsequent to the invasion of Ukraine, the U.S. continues to be in a nervous waiting game as the real threat of Putin to act (cyber or otherwise) inside the domestic landscape of the U.S.

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

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

The U.S private sector, academia, research and development entities, and our core fabric of ideation has become the geopolitical battlespace for China.

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

DATA AS A COMMODITY

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

China's ability to holistically obtain our Intellectual Property and Trade Secrets via illegal, legal, and sophisticated hybrid methods is like nothing we have ever witnessed. Joint ventures, creative investments into our federal, state and local pension programs, collaborative academic engagements, Sister City Programs, Confucius Institutes on Campus, Talent Recruitment Programs, investments in emerging technologies, and utilization of front companies continue to be the framework for strategically acquiring the thoughts and ideas of our researchers, as well as development of those ideas pre and post patent application. The threat from China pertaining to academia is both wide, and deep. The past four 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.

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

The proverbial salt in the wound of all this nefarious activity is when the CCP steals our thoughts, ideas, patents, and technology, and manufactures that same technology in China, and the sells it back to American companies and around

the world. One needs to look no further than the American Supercomputer Corporation for just a glimpse of the long-term impact to economic espionage. Then one must factor in all the manufacturing plants which were not built, and the tens of thousands of jobs which were not created because China, via its theft, beat the U.S. to the global market and is selling the same product and a significant reduction in real costs.

As I stated earlier in this statement, the passage of the CHIPS and Science Act is a seminal moment in our nation's history, particularly as it pertains to the critically of a vibrant, and real, partnership between corporate America and the U.S. Government. This partnership is imperative if the U.S. will continue to lead and compete at a high level against the CCP in a competitive economic war.

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.

CHINESE NATIONAL LAWS ASSIST DATA COLLECTION

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

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

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

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

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

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

Hence, if you are a U.S. business seeking to enter a business relationship with a company in, or from, China, your data will be obtained and provided to the MSS or PLA for their usage. This includes third party data as well. The analogy is a U.S. company enters into a business deal or partnership with a company from another country. The U.S. company must provide all relevant and requested data from their company, as well as the partner company, to the NSA, CIA and FBI.

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

UNEQUAL PLAYING FIELD

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. The world has seen recently what the CCP is capable of when one of the largest companies in the world, Alibaba, pushes back on state-run efforts.

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

Hence, for a prospective business deal with a company in the U.S., the Chinese company can partner with China's intelligence services to assist in negotiations, vulnerabilities, and utilization of any already acquired data from said U.S. company. Again, this is akin to a U.S. based company calling 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.

OPERATIN FOX HUNT

In furtherance of the CCP's influence efforts, Operation Fox Hunt is an insidious international effort by the CCP to identify, locate and attempt to bring back Chinese dissidents who have left China and are causing President XI and the Communist Party discontent. For almost a decade Chinese intelligence services have been building teams to conduct surveillance in the U.S., oftentimes falsely

enter relationships with local law enforcement to garner information on who China claims are fugitives, and attempt to bring them back to China.

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

CYBER AS A NEFARIOUS TOOL

As stated previously, the CCP has significant and unending resources to penetrate systems and obtain data, or sit dormant and wait, or to plant malware for future hostilities in organizations, infrastructure, and academic institutions. Over the past decade we have seen CCP cyber breaches, activity, and successes and criminality to such a level I fear we are becoming numb when it is identified. One such event was the Equifax breach in May of 2017. As former head of U.S. Counterintelligence, I consider this to be one of the CCP's greatest counterintelligence collection successes. More than 145 million Americans had all their financial data, nicely aggregated, to the CCP along with Equifax's trade secrets on how they acquired such data. That is every American adult. Anthem lost 80 million medical records in 2015, Marriott lost 500 million guest's records in 2014, and in 2015 OPM lost 21 million records to China's cyber theft. I would be remiss if I left out China's breach of multiple cloud service providers in which China obtained access to over 150 companies' data. Their cyber success in the U.S. is painful and persistent. We must do more to protect our data and be vigilant in elimination of self-inflicting wounds.

CHINA AND INSIDER THREAT AND MALIGN INFLUENCE

The Insider Threat epidemic originating from the CCP has been nothing short of devastating to the U.S. corporate world, research institutions and academia. Anyone can go to Department of Justice's web site and search economic espionage. The result is hard to accept. And those listed cases are just what was identified, reported by a U.S. company, and then prosecuted. From General Electric, Harvard, MIT, and countless other victim organizations, data loss, ideation and technological advancement, as well as brand are just a few of the consequences.

When you combine the persistence of intent and capability for the CCP's cyber intrusion programs, with the onslaught of Insiders being arrested, indicted and convicted by the FBI and DOJ over the past decade, it creates a formidable mosaic of insurmountable levels.

I would be remiss if I did not reference the strategic and aggressive nature in which the CCP conducts malign foreign influence in the U.S. Unlike Russia's persistent attempts to undermine our democracy and sew discord, mostly at the federal level and within the U.S. Congress, the CCP strategically, and with precision, conducts nefarious influence campaigns at the state and local level. The ability, and success of the CCP to lobby and provide economic enhancements to influence policy and investment at the local level is strategic and sometimes invisible to the untrained eye. We much identify this activity and provided local officials tools to make risk-based decisions prior to engaging in multi-million-dollar agreements.

CONCLUSION

In closing, I would like to thank this committee, and the Senate writ large, for acknowledging the significant counterintelligence threats to our corporate ecosystems and academic and research institutions., not only by holding this hearing, but with all the recent legislative actions the past year on combatting this threat as well as driving enhanced competition. Continuing to combat the threats to our nation 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.

Regarding these awareness campaigns, we must be specific and reach a broad audience, from every level of government to university campuses, from board rooms to business schools, educating on how China's actions impair our competitive spirit by obtaining our research and development, trade secrets and intellectual property, and degrading our ability to maintain our role as economic global leaders. I have provided some recommendations for this committee, the IC, the administration, academia, research and development, as well as CEOs and board of directors in our holistic efforts to detect and deter these threats, as well as educate, inform, and compete. Our nation needs strategic leadership now more than ever, particularly when we face such an existential threat from a capable competitor who is looking beyond competition to the global dominance.

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

China, particularly with respect to the long-term existential threat is hard to see and feel, but I would suggest it is much more dangerous to our viability as a nation.

Recommendations:

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

1. Conduct a comprehensive analysis of the modern counterintelligence threat landscape and potentially enhance authorities, capabilities, and organization structures to most effectively protect our government, private sector, and academia. This should include the critical evaluation of counterintelligence, and intelligence, resources assigned, and dedicated, to the FBI, Intelligence Community agencies, and other counterintelligence organizations to identify existing gaps in coverage, authorities, and modern approaches to protecting our nation form hostile nation states.

2. Enhanced 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 authorities and economic councils to enable risk-based decision making on investments and partnerships with foreign entities. The analogy would be the Financial Services ISAC, on steroids. This intelligence analysis and delivery mechanism should include the Intelligence Community, FBI, CISA, and select members of the non-Title 50 ecosystem. The core constituency should be state and local entities, corporate organizations, and academic institutions at risk form foreign adversaries. Existing vehicles such National Governors Association and the Chamber of Commerce can be utilized to increase threat awareness of illicit activities investment risk at the state and local level.

3. Declassification of real time and actionable intelligence. The Senate must ensure the FBI, CISA, and the Intelligence Community are leaning aggressively forward in providing collected intelligence pertaining to nation state plans and intentions, as well as illegal and legal activities, in software, coding, supply chain and zero-day capabilities. The U.S.

Government must be more effective in providing intelligence to the private sector. Enhanced declassification of collected intelligence with respect to threats to our economic well-being, industries, and companies must be delivered at speed to impacted entities prior to the threat becoming realized.

4. Ensure implementation of the legislatively proposed Malign Foreign Influence Center. Ensure the private sector and big tech will be a constituent of the intelligence derived. This effort becomes more critical as we approach the mid-term elections and only two years form a Presidential election.

5. Expanded bipartisan congressionally led "China Threat Road Shows" to advise and inform the counterintelligence threat to CEOs, Governors, and Boards of Directors in critical economic, research and manufacturing sectors.

6. Executive branch prescriptive requirements, with governance and oversight, of the CHIPS and Science Act and Inflation Reduction Act implementation with reporting requirements of both the government and private sector entities engaged in spending the appropriated monies as well as developing the technologies associated, particularly in the research and development space. This effort must be either an Executive order or legislatively directed, or it will not occur.

7. Create a panel of CEOs who can conversely advise and inform Congress, FBI/CISA and 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. This can be accomplished by resourcing NCSC to reconstitute the NSBAC and NSHEAB as referenced earlier.

8. 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. Enhancement of NCSC's resources can effectively function in this capacity if addressed, appropriated, and allocated appropriately.

9. 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, the Federal Thrift Savings Plan, land and property purchases in the U.S. and the proliferation of ZPMC crane ensembles at numerous port critical to the supply chain of commerce, and our military.

10. Immediately create a Supply Chain Intelligence function which can sit both in the Intelligence Community as well as outside to facilitate real time intelligence sharing. This entity should include members of the private sector skilled in understanding our supply chain and who can expedite reacting to emerging threats. This entity will also be able to provide the U.S. Government cogent mitigation strategies and assistance with policy formulation to protect our vulnerable supply chain from persistent penetration and manipulation by China and Russia. The partnership between the IC and non-Title 50s must be enhanced to accomplish this critical aspect of securing America's supply chain.

11. Reevaluate the budgetary process for appropriation of funding to combat foreign nation state adversaries. This should include enhanced budges with explicit and direct funding/resources to address counterintelligence related matters and shortfalls outside the historical aspects of counterintelligence (Supply Chain, Critical Infrastructure).

12. The Administration should create an Executive Order, or via legislative action, direction of non-title 50 entities to establish and resource fundamental counterintelligence programs within their agency. This effort should be analogous to the CIO or CISO organizations currently existing which coordinate with the Federal CIO.