S. HRG. 117–599

OPEN HEARING: ON PROTECTING AMERICAN INNOVATION: INDUSTRY, ACADEMIA, AND THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 21, 2022

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

50–083 WASHINGTON : 2023

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong. 2d Sess.]

MARK R. WARNER, Virginia, *Chairman*
MARCO RUBIO, Florida, *Vice Chairman*

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
MICHAEL F. BENNET, Colorado
BOB CASEY, Pennsylvania
KIRSTEN E. GILLIBRAND, New York

RICHARD BURR, North Carolina
JAMES E. RISCH, Idaho
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
TOM COTTON, Arkansas
JOHN CORNYN, Texas
BEN SASSE, Nebraska

CHUCK SCHUMER, New York, *Ex Officio*
MITCH MCCONNELL, Kentucky, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*
JAMES INHOFE, Oklahoma, *Ex Officio*

MICHAEL CASEY, *Staff Director*
BRIAN WALSH, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

SEPTEMBER 21, 2022

OPENING STATEMENTS

	Page
Warner, Hon. Mark R., a U.S. Senator from Virginia	1
Rubio, Hon. Marco, a U.S. Senator from Florida	4

WITNESSES

Evanina, William R., Founder and CEO, Evanina Group; Former Director, National Counterintelligence and Security Center	5
Prepared Statement for the Record	7
Van Cleave, Michelle, Senior Advisor, Jack Kemp Foundation; Former National Counterintelligence Executive	24
Prepared Statement for the Record	26
Gamache, Kevin, Ph.D., Associate Vice Chancellor and Chief Research Security Officer, Texas A&M University System	40
Prepared Statement for the Record	42
Sheldon, Robert, Director, Public Policy & Strategy, Crowdstrike	47
Prepared Statement for the Record	49

SUPPLEMENTAL MATERIAL

Answers to questions for the record from Michelle Van Cleave	76
Answers to questions for the record from Kevin Gamache	90
Answers to questions for the record from Robert Sheldon	97

OPEN HEARING: ON PROTECTING AMERICAN INNOVATION: INDUSTRY, ACADEMIA, AND THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

WEDNESDAY, SEPTEMBER 21, 2022

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:44 p.m., in Room SH–216 of the Hart Senate Office Building, Hon. Mark R. Warner, Chairman of the Committee, presiding.

Present: Senators Warner, Rubio, Feinstein, Wyden, Bennet, Casey, Collins, Blunt, Cotton, Cornyn, and Sasse.

OPENING STATEMENT OF HON. MARK R. WARNER, A U.S. SENATOR FROM VIRGINIA

Chairman WARNER. Good afternoon. I'm going to call this hearing to order. And I want to welcome to our nongovernment expert witnesses, although at least two have served with distinction in the government.

Let me start with the Honorable Bill Evanina, former Director of the National Counterintelligence and Security Center. He's also the founder and CEO of the Evanina Group.

The Honorable Michelle Van Cleave, senior adviser, Jack Kemp Foundation, and again, former National Counterintelligence Executive at the Office of Director of National Intelligence.

Dr. Kevin Gamache, who is the Vice Chancellor and Chief Research Officer at Texas A&M University System.

And Mr. Robert Sheldon, the Director of Public Policy and Strategy at CrowdStrike.

Today's hearing, "Protecting American Innovation: Industry, Academia, and the National Counterintelligence Security Center," will examine the implications of the findings of our Committee's bipartisan report on the NCSC, which we publicly released yesterday.

This is the first in a series of hearings on the report. Future hearings will include current U.S. counterintelligence officials to discuss, in more depth, concrete changes that may be necessary for the NCSC and the government's counterintelligence enterprise.

I think we all understand that the traditional model of intelligence that evolved post-World War II and, in many cases, in our country and countries like the U.K., evolved a long time earlier, particularly post-World War II, when we, the Brits, the Russians had a series of espionage agents oftentimes working out of an em-

bassy and basically trying to discover information or secrets about a foreign adversary. That classic spy-versus-spy model is pretty much in the historic dustbins at this point. As I think we know, our Nation now faces a dramatically different threat landscape than it did even a couple of decades ago. Today's foreign intelligence threats are not just obviously targeting the government but are increasingly looking at the private sector to gain technological edge over industries.

One of the remarkable statistics is that as much as $600 billion of intellectual property is stolen each year from the United States. And that doesn't even count what's stolen from some of our allies and partners around the world. New threats and new technologies mean that we need to make serious and substantive adjustments to how we address the issue of counterintelligence if we are to protect America's national and economic security.

For many years, Members of this Committee were constantly hearing the alarm bell ringing when we got briefings on these foreign intelligence threats. We felt it was important not just to be made aware of that threat but to also do something about it. So, I want to thank Senator Rubio, Senator Cornyn—I think Senator Cotton appeared—and Members on my side of the aisle, where we went out, and oftentimes with Bill Evanina, did what we called a series of classified roadshows to focus particularly on the challenge and nontraditional means of espionage put forward by the PRC.

We did that with tech companies, we did it with VCs, and we did it in academia, again, to really look at the challenge presented by the CCP and the leadership of Xi Jinping. As I mentioned, we did aerospace, advanced manufacturing, artificial intelligence, biotech, data analytics—a whole host of areas where we are now engaged in a tremendous competition. We started to take action on that competition.

I'm proud of the fact that, in a broadly bipartisan way, there is now a law to make sure that we can bring part of that semiconductor industry back to the United States. My belief is there may be other technology domains where we have to make similar investments, because clearly, we know that the CCP is making these investments.

I was an old telecom guy and it was more than stunning to me when it became clear that not only had the PRC suddenly obtained the leading international company in 5G in the form of Huawei, but that they were also setting the rules, standards, and protocols for that emerging technology. FBI Director Wray has stated the bureau literally opens up a new PRC-related counterintelligence investigation every ten hours. Thousands of these cases are open. China has stolen more American personal and corporate data than every other nation in the world combined.

With this hearing, we are broadening our counterintelligence focus to also look at the malign role played by other large state adversaries like Russia, as well as Iran, North Korea, and other states. However, as we discuss what the CCP in particular is doing in the United States, I want to make myself crystal clear that my concern lies squarely with Xi Jinping and the Chinese Communist Party, not the people of China and certainly not with Chinese or Asian-Americans or any parts of the Chinese diaspora anywhere in

the world. Matter of fact, failure to make that distinction oftentimes will play right into the CCP's propaganda agenda. And many times, it is Chinese-Americans who are the victim of the CCP's intelligence service activities. Similarly, we've recently seen those brave Russians who came out at some level of force to protest against Vladimir Putin's war. We saw the arrest of the opposition leader, Navalny. Again, our beef is not with the Russian people or immigrants of Russian descent but with the kleptocratic and murderous regime of Vladimir Putin.

The Committee's report is the product of years of independent research by nonpartisan Committee staff to assess the mission, authorities, and resourcing of the NCSC and its mission to coordinate the government's counterintelligence efforts.

Among the report's findings are: one, that the United States faces threats from a wide variety of adversaries, including powerful state rivals such as China and Russia, regional adversaries, minor states, and the organizations that play out these entities' operations, oftentimes not simply within the traditional spy services. Foreign intelligence entities are targeting a wide set of public and private entities, including U.S. government departments and agencies that are not part of the Intelligence Community and not part of our national labs or other traditional sources. But they are going after the financial sector, our energy sector, and a lot of folks in the industrial base and academia.

Today's adversaries have access to a much wider variety of tools for stealing information, influencing U.S. officials, or inflaming social and political tensions than in the past, including nontraditional human, cyber, advanced technical, and other source Intelligence operations to collect against U.S. plans and policies, sensitive technology, and personally identifiable information. How we make sure we protect that as well as our intellectual product in this country is part of our responsibility in this Committee. Despite the wide-ranging and sophisticated number of counterintelligence threats facing the U.S., the United States counterintelligence enterprise is not postured to confront the whole-of-society threat facing the country today, with the NCSC lacking a clear mission as well as sufficient and well-defined authorities and resources to effectively deal with this.

Now, I'd love to say that report came up with a series of specific recommendations. It did not. I think it posed a number of the problems, but this hearing and others is how we get at this issue. And we clearly have folks who played from inside the government role, on the IC side, and outside experts as well.

So the core questions for this hearing are: what role should academia and industry play in protecting information with national security implications? Are there legislative or policy changes needed to codify that role? What government resources may be needed to help academia and industry protect their data technologies and people? And what role is the NCSC, as the lead agency for national counterintelligence, expected to play in informing and coordinating with all of these entities? Given the increasingly important role of counterintelligence—due to the threats from these foreign governments—I think I have some real questions about this, I know.

The report posited the question, does the U.S. government need an independent counterintelligence agency to tackle them? I have some doubts about that. While no consensus, as I mentioned, has been raised, we're going to look at this problem in a comprehensive way. And we welcome not only the panel but others' input into this determination.

The truth is the intelligence traditions have changed dramatically from the postwar era, from the Cold War era. We are engaged, particularly with the PRC, but with others as well, in a technology competition that will define who becomes the security and economic leader of the 21st-century. It's my hope that America maintains that leadership role. But to do that, we've got to have an effective counterintelligence operation.

And with that, I turn to my friend, the Vice Chairman.

OPENING STATEMENT OF HON. MARCO RUBIO, A U.S. SENATOR FROM FLORIDA

Vice Chairman RUBIO. Well, thank you, Mr. Chairman. Thank you all for coming here today. I think you've covered most of it. And I think our Audits & Projects team has done a good job of identifying the problem. And part of these hearings is now to begin to think through what are some of the things that we can do from our end to either mandate or provide a pathway toward solutions.

The core problem is this—and you've stated it well—the way I would describe it, in general, is: our entire system is set up for an era in which counterintelligence, basically espionage, was governments trying to steal government secrets. Getting into the Defense Department, learning about things that have to do with nation-state proprietary information and classified information. We're now in an era in which the activities of intelligence agencies from around the world come from a variety of countries with different intentions. They range from cyber intrusions designed to both steal secrets and also to generate revenue to disinformation and misinformation to try to steer and influence and shape American policy and divide us and distract us or debilitate us to, obviously, academia, both because they're interested in research, but frankly, in many cases, to try to influence students.

It's a long-range plan to look at someone who's 20 years old today and say we can shape their narrative about China and Taiwan, or China and Tibet, or China and Uyghur Muslims in Xinjiang. Twenty years from now, these individuals will be running companies or key agencies in government—and maybe even elected—and that will help us. This is a multifaceted, new-era type challenge, which our agencies simply weren't created to address. They were created in an era where there wasn't great power competition, where the number of nations around the world that had the capability to even do intelligence operations against the United States domestically, not to mention globally, was much smaller than it is today.

So, really, the hope here today is to understand how we can help clarify the mission, particularly of the National Counterintelligence and Security Center, the NCSC. How we can give it a clear mission that captures the full array of challenges, provides them with well-defined authorities that allow them to do that, and then under-

stand whether or not we're providing sufficient resources to be able to carry that out?

And those three things, having the clear mission, having the authorities to carry out the mission, and having the resources to carry out that mission are the path forward. But it really begins with understanding a clear mission as to what it entails and all the intricacies and complications that would come with that.

All of you have been involved in different ways with this, and we're grateful you came in today to help us begin to chart the way forward.

Chairman WARNER. And thank you, Vice Chairman Rubio. I'm proud of the staff work that put together this report. The tradition of this Committee is that we do things bipartisan. This at least gives a roadmap of what some of the issues are. Now, we're looking to sort through what the answer should be.

So, I want to start, Bill, with you, and we're going to go left to right down the panel.

STATEMENT OF HON. WILLIAM R. EVANINA, FOUNDER & CEO, EVANINA GROUP; FORMER DIRECTOR, NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Mr. EVANINA. Chairman Warner, Vice Chairman Rubio, Members of the Committee, it's a pleasure. Humbled to be back here in front of you in this Committee, especially with an esteemed panel of experts here today.

I want to first thank the Committee and the Members of the Committee for your continued leadership commitment to the Intelligence Community, law enforcement, and the dedicated women and men around the globe keeping us safe and free.

Our enduring democracy and unsurpassed economy, along with the best military in the history of the world, affords us with fundamental and unparalleled freedom and security. Protecting those freedoms and security are in some part due to those dedicated women and men serving in the counterintelligence arena.

However, the job has never been more difficult than it is today. The threat landscape has dramatically expanded in the past decade, specifically with the counterintelligence battlespace transitioning to the private sector, especially with respect to the Communist Party of China. The past decade has also provided us with a very clear mosaic of the modernization of the nation-state threat actors conducting persistent, strategic, and sometimes destructive cyberattacks on American government agencies, corporations, and academic institutions. Their data, their systems, and their employees have all been targeted. Strategically-placed insiders in cyber penetrations are the most commonly utilized modalities of the Communist Party of China. With 21st-century asymmetric threats increasing exponentially, it is time to take an honest, modern, and reimagined view of counterintelligence.

Counterintelligence is not just catching spies or insiders from adversarial countries, but also, it is a key defense mechanism of our Nation's key source of strength and posterity: our economy. We must also approach counterintelligence with the same sense of urgency, spending, and strategy 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 action. As much as counterintelligence investigations, strategy, and policy are inherently government functions and responsibilities, U.S. corporations, research institutions, non-Title 50 organizations, and academia must become a larger part of the process of protecting their own proprietary data, trade secrets, and fundamental research. China and others are attempting every day to take what they ideate and develop. This is especially true when such organizations receive federal grants and funding. 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 existing and extensive funding provisions and technological incentives provided by these legislative actions.

I would offer emerging renewable energy technologies and semiconductor production will be targeted the most aggressively by China. From a counterintelligence perspective, where does this protection responsibility reside? This is a counterintelligence issue. Ten years from now, this Committee cannot be holding hearings and asking how China stole our federally-funded and -subsidized capabilities and secrets and progress, and then selling them back to us as customers.

I would like to close by acknowledging that defending our Nation, especially in the counterintelligence arena, has become complicated and encompassing. However, I would be remiss if I did not mention the United States possesses the finest offensive capabilities and counterintelligence personnel the world has ever seen. As this Committee is fully aware, their dedication, their successes are impactful. They're enduring, and they properly remain silent. Our Nation is grateful.

Thank you for the opportunity to be here today, and I look forward to your questions.

[The prepared statement of Hon. Evanina follows:]

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.

STATEMENT OF HON. MICHELLE VAN CLEAVE, SENIOR ADVISOR, JACK KEMP FOUNDATION; FORMER NATIONAL COUNTERINTELLIGENCE EXECUTIVE

Ms. VAN CLEAVE. Mr. Chairman, Vice Chairman Rubio, Members of the Committee, let me begin by echoing the praise that my colleague, Bill, has just iterated for our counterintelligence professionals. It was my honor to have served as the Director of Senate Security from 2020 to 2021. So, I feel warmly at home appearing before you here today.

I was also deeply honored when President George W. Bush appointed me the first statutory head of U.S. counterintelligence. That position, as you know, was created by the Counterintelligence Enhancement Act of 2002, which was, as it happens, voted out of Committee 20 years ago next week—voted out of the Senate, rather—20 years ago next week under the careful leadership of this Committee.

I believe that your leadership is sorely needed again. Mr. Chairman, to that end, I have prepared a written statement which I hope may be of help to you, and I ask that it be included in the record.

Chairman WARNER. So ordered.

Ms. VAN CLEAVE. Foreign powers use their intelligence capabilities to advance their goals and to prejudice ours. In today's volatile geopolitical environment, their operations are intensifying against us, not waning. Russia's war on Ukraine has changed everything, setting the stage for what President Biden has called a battle between democracy and autocracy.

Having lived through the events of January 6 with all of you, I am acutely aware of the lines of fragility in our democracy, which foreign powers have and will continue to seek to exploit. The bottom line I would offer is this. The core counterintelligence mission to identify, assess, and defeat foreign intelligence operations has never been more crucial to U.S. national security. Protective security plans and programs, to be sure, are profoundly important. And I have little doubt that we are all agreed on that point. But they will never be enough. In my view, the United States cannot afford to cede the initiative to those who are working against us. The stakes are too high.

Indeed, the old wisdom is still true: the best defense is a good offense. But unfortunately, our counterintelligence enterprise has never been configured to be able to preempt. Preemption requires strategic national planning and coordinated operations against foreign intelligence threats. By contrast, our CI agencies have very distinct and separate missions, and they operate within their own lanes. And each is very good at what they do, but as experience has shown, that is not enough. These are the very deficiencies that the CI Enhancement Act of 2002 intended to correct.

However, while the law back then created a national CI mission to integrate CI activities, it did not create the means by which that could be carried out. So, the first National Counterintelligence Strategy, which was issued by President Bush, called for creating a strategic CI capability to proactively disrupt foreign intelligence threats, starting with working the target abroad. Where are they situated? How do they recruit? Who are their personnel? What are

their liaison services? How are they tasked? What are their vulnerabilities? How can those vulnerabilities be exploited? There was a pilot program to do that on a select high-priority target that was started under my watch with congressional support. But it was quietly terminated after I left.

Subsequent national counterintelligence strategies have omitted this key goal altogether, and the national office has moved on to do other things. So, we've been stuck in neutral for 20 years. To date, neither strategic counterintelligence nor a strategic CI program is defined in law or anywhere else. The very concept of a national counterintelligence mission, different from what the operating arms are already doing, was and remains new and untested.

Without the discipline of a national program, our CI management will continue to measure performance against the individual agency metrics for which they are accountable, as they must. But is that enough to counter the foreign intelligence threats directed against the United States? I fear that scorecard may be very much in doubt, which I hope the Committee will choose to explore in greater detail as part of your much-needed oversight of U.S. counterintelligence and this series of hearings.

As for the national mission and office, I think this Committee had it right 20 years ago. The challenge still remains how to pull together a strategic counterintelligence program: one team, one plan, and one goal. Your leadership and some carefully crafted clarifying amendments to that 20-year-old law could make all the difference.

I look forward to your questions.

[The prepared statement of Hon. Van Cleave follows:]

Michelle Van Cleave
Statement for the Record
Senate Select Committee on Intelligence
Hearing on Protecting American Innovation:
Industry, Academia and the National Counterintelligence and Security Center
September 21, 2022

Chairman Warner, Vice Chairman Rubio, Members of the Committee:

I am very grateful for this opportunity to present my views on the national counterintelligence mission and the office that Congress established, 20 years ago, to lead U.S. counterintelligence (CI). Based on my experience as the first person to serve in that office, and my continuing engagement in the field, I have three conclusions to submit for your consideration:

- Judging by the record, the national CI office has failed to accomplish the principal goals for which it was created.[1] While there are many factors at play, the most significant in my view is the lack of consensus on what those goals are. As a consequence, the U.S. counterintelligence landscape is still struggling with many of the difficulties this Committee identified 20 years ago – along with some new ones laid bare by the upsurge in malign influence operations directed against our democracy.
- I am convinced these deficiencies can be remedied. With the benefit of hindsight and lessons learned over the last two decades, the time is ripe for some clarifying legislation. I know that your investigative staff has been hard at work on that task. To that end, I would like to offer some ideas, for the Committee's consideration:
    - To define, in law, "strategic counterintelligence" and the related mission assigned the head of U.S. counterintelligence; and
    - To establish a strategic CI program – budgets, billets, authorities, and accountability -- by which that mission can be accomplished.
- Security measures alone, while vitally important, will never be enough. Without a renewed emphasis on the core business of U.S. counterintelligence, the United States will continue to forfeit the initiative to foreign adversaries and suffer costly losses to growing hostile intelligence threats.

Significance of the Counterintelligence Enhancement Act of 2002

Despite a history of damaging CI failures, U.S. counterintelligence has been largely immune from reorganization schemes because it never had a conscious organization plan to begin with. The National Security Act of 1947 established the basic contours of the post-war U.S. intelligence community, but (apart from defining the term[2]) said nothing about counterintelligence.

Unlike most modern nation-states, the United States has never had a national counterintelligence "service." Instead, CI operational authority was split in gross terms

between the needs of domestic security (assigned to the FBI), and the operational needs of intelligence collection (assigned to CIA) and military operations/force protection in the field (assigned to DoD and the military services). There was no overarching national leadership to provide cohesion or strategic direction for America's CI activities.

Twenty years ago, Congress took a look at the enterprise and saw that it was little changed from the set pieces that emerged after World War II. The lead operational agencies each had a vital CI mission shaped and executed as part of their own organizational responsibilities. But they had the barest understanding of what resources and capabilities the others possessed, much less their operational, analytic, or resource plans beyond the current budget year; or how "foreign intelligence threat" was defined or assessed beyond their own area of responsibility.

There were no agreed guiding principles or CI doctrine across the discipline, nor a standard approach to targeting, much less a coherent joint strategy or national program to disrupt hostile intelligence operations. Given the extremely close-hold nature of counterintelligence, interagency information sharing was poor, and infrastructure support even worse. Even the modest national mechanisms developed to deconflict offensive CI activities stopped at the water's edge, a legacy of the old divide between foreign and domestic operational realms. And there was no shared concept of a national or strategic version of the CI mission.

As a consequence, no one had a common operating picture of the foreign intelligence threats arrayed against the United States, or (equally important) the "blue side" forces available to counter those threats. With three operating elements, each with differing missions, responsibilities, and resources, all the incentives were to address agency-specific matters, case by case, rather than to work as one team to identify and counter hostile intelligence threats to the United States. Where coordination was required by policy, it was for the purpose of deconflicting the tactical environment rather than supporting strategic objectives.

Taken together, this inchoate architecture of U.S. counterintelligence has been costly. Foreign powers have rigorously leveraged the resulting gaps in the U.S. CI framework, especially as they presented opportunities in relatively non-hostile, third country operational environments. Adversary intelligence services found they could exploit DOD's dependent authorities to conduct counterintelligence for an other-than-force-protection purpose, overwhelm CIA's limited CI resources, and take advantage of the FBI's constrained ability to work abroad.

Congress decided it was time to put someone in charge of the enterprise.

The *Counterintelligence Enhancement Act of 2002* established in law a national head of U.S. counterintelligence, who would be responsible for providing strategic direction and integrating the activities across U.S. counterintelligence. Drawing on an in-depth Clinton-era interagency study ("CI-21") and ensuing Presidential Directive (PDD-75), the purpose was twofold:

- First, to close the seams that existed between the fiefdoms of the several operating agencies, which were being exploited by spies seeking a way into U.S. national security secrets, to devastating effect.[3]

- The second, over-arching purpose was to develop and execute a national-level counterintelligence strategy to protect the United States against foreign intelligence threats.

The *Counterintelligence Enhancement Act,* together with "CI-21," represented a conceptual breakthrough in American counterintelligence. They judged that the central strategic core that is needed to identify, assess, and defeat foreign intelligence threats to the United States and its vital interests had been missing. This is the fundamental flaw in the architecture of U.S. counterintelligence which the new national office was created to remedy -- not by its mere existence, but by leading the transformation and strategic integration of our Nation's CI capabilities.

And that is where the new office has fallen short.

First National Counterintelligence Strategy and its aftermath

9/11 taught us a hard lesson. It is not acceptable to wait until the terrorists are here in our own backyard, where we are most vulnerable and at risk. The objective must be to find them, and stop them, before they can strike. That requires identifying and assessing their "order of battle" – their training camps, hiding places, headquarters' cells, support networks, recruitment nets, logistics infrastructure, targeting plans, etc. Based on this now well-understood target set, operational plans can be developed to exploit their vulnerabilities, including the execution of carefully orchestrated pre-emptive actions when so directed.

There were lessons here for U.S. counterintelligence. In the past, America's default CI strategy has been to wait to engage the foreign intelligence adversary in our own backyard, rather than in theirs. Over half of the U.S. CI budget post-World War II has been devoted to activities within the United States carried out by the FBI. In addition, most of the remainder allocated to CIA, the Defense Department, and to small pockets elsewhere in the government, has gone to programs and personnel based wholly or in part within U.S. borders. The result of this insular posture? A long history of devastating losses to espionage and other hostile intelligence operations. Something had to change.

Go on the Offense

As Jim Olson, former head of counterintelligence at CIA, explains in his classic article *The 10 Commandments of Counterintelligence*, "CI that is passive and defensive will fail... Our CI mindset should be relentlessly offensive. We need to go after our CI adversaries."[4] While this imperative has long been understood and practiced at the tactical level, its application as declared national-level strategy was not.

The first *National Counterintelligence Strategy*, issued by President Bush in 2005, was a sharp departure from the past. Rather than wait until the foreign intelligence threat is here, at our doorstep, the *Strategy* directed that U.S. counterintelligence go on the offense, to exploit where we can, and interdict where we must, with the purpose of degrading the adversary service and its ability to work against the United States.

Executing an offensive national CI strategy begins with working the target abroad. How are foreign intelligence personnel recruited, trained, tasked? Who are their leaders, reporting chains, liaison relationships? Where do they operate? How? What are the gaps in our understanding? How can we gain the insights and capabilities we need to identify and exploit adversary vulnerabilities? As directed by national security priorities, the considerable resources of the members of the U.S. intelligence community that have global reach would be directed to help identify and then neutralize or exploit the intelligence activities of foreign adversaries. One team, one plan, one goal.

The need for this capability was driven home in America's experience with the war against Iraq. In the lead-up to "Operation Enduring Freedom," an interagency CI strategic planning team came together to develop a common operating picture of Iraqi intelligence operations worldwide. In response to Command Authority direction, the "Imminent Horizon" team was chartered to render Iraqi intelligence ineffective. While this effort resulted in some important successes, the CI community learned its lessons the hard way.

Strategic operational planning to degrade foreign intelligence capabilities has long lead times. Beginning at D minus 6 months – as was the case with Iraq – is too little too late. Even though Coalition Forces had technically been at war with Iraq for ten years, flying daily combat missions, the CI community could identify and contain an unacceptably low percentage of Iraqi intelligence assets.

The Iraq war after-action reports confirmed, once again, the compelling need for standing joint strategic planning, for building interoperability across CI agencies, and for proactive operations to degrade foreign intelligence threats. But here we had a problem. The U.S. CI enterprise was not designed to pre-empt.

The CI enterprise was neither configured to serve a strategic purpose, nor postured globally to disrupt a foreign intelligence service. Apart from wartime, the U.S. government has not routinely addressed foreign intelligence capabilities as part of a national security threat calculus informing national strategy and planning. Given this benign neglect, U.S. CI capabilities are tailored to meet agency- specific needs, but not designed to operate jointly.

While one of the inherent strengths of U.S. counterintelligence is the diversity of skills, methodologies and resources across the profession (in contrast to a single national service, such as MI-5), there was neither process nor infrastructure to marshal them to common end. And such disunity leads to an inherent weakness: seams that adversaries could exploit.

In short, the whole was less than the sum of its parts. That needed to be fixed.

New CI Business Model

To that end, the Bush *Strategy* called for a new business model for the CI enterprise, to provide the strategic coherence to go on the offense against select targets. The goal was to create an additional CI capability at the national level, in service of a new and interdepartmental mission that would address the increasing success of the intelligence services of foreign powers in their exploitation of the 'gaps' described above.

Conceptually, this undertaking consisted of two parts: first, a global CI assessment of foreign intelligence presence, capabilities and activities; and second, a CI "doctrine" – the fundamental principles that guide military or other operations in support of national objectives -- for attacking adversary services systematically via strategic CI operations. At home, the proactive CI mission called for a coordinated, community-wide effort of aggressive operational activity and analysis to obtain the intelligence necessary to neutralize the inevitable penetrations of our government.

National teams, consisting of representatives from key CI components, would be responsible for this centralized strategic planning against designated high-threat foreign intelligence adversaries. Upon the direction of the NCIX, departments and agencies would pre-obligate certain of their resources to the new national program (or acquire new resources as approved by Congress) sufficient to meet their new obligations under the *Strategy*. Operational responsibility for distributed execution was assigned to the FBI, CIA, or DoD as appropriate, each of which would retain budget and program control over their respective CI activities.

Based on this model, and with Congressional support, we initiated a pilot program against a high priority target.

Just as this work was getting underway, major change was sweeping across the U.S. intelligence community: the creation of the office of the Director of National Intelligence (DNI). Authority and responsibility for overseeing CI budgets, collection and analysis, previously under the NCIX, became part of the portfolios of the various DNI functional deputies. The pilot strategic CI program ran into stiff resistance, especially from CIA, which was straining to meet all of the extra staffing requirements imposed by the numerous new DNI centers, directorates and mission managers.

After I left office, I learned the pilot program had been terminated, the group's funding and a related mission transferred to the National Clandestine Service at CIA. The experiment in national strategic integration came to an abrupt end. As before, individual department and agency priorities would take precedence over any national level CI effort. And they in turn would have to compete with other national priorities for funding and attention.

The fatal flaw

The *Counterintelligence Enhancement Act* and the standup of the NCIX should have heralded a new chapter in U.S counterintelligence, enabling the strategic direction and integration of U.S. counterintelligence capabilities to common end. So why did it all fall apart?

As envisioned by the *Counterintelligence Enhancement Act*, the President issued a strategy to array U.S. counterintelligence activities to a common purpose. The express intent was to create a strategic CI capability to identify, assess, and proactively disrupt foreign intelligence threats to the United States. But there was no means of carrying that out.

Effective integration and coordination across the interagency require the discipline of a national program: budgets and billets and authority and accountability to meet defined ends. It is not enough to exhort cooperation through national guidance or interagency meetings. Even strong national leadership, charismatic personalities and popular ideas will falter absent the

institutional tools that drive, capture and internalize the results needed to enable strategic coherence.

Yet in establishing the NCIX as the head of U.S. counterintelligence, the law did not create a corresponding national CI program by which the strategic integration of U.S. CI capabilities could be accomplished. Subsequent national CI strategies have omitted this seminal goal altogether. Funding and resources devoted to traditional CI targets have continued to decline in the face of competing priorities, while the office of the NCIX (now the NCSC, as discussed below) has turned its attention to other concerns.

As a consequence, U.S. counterintelligence has been stuck in neutral for 20 years now while the threats — and our vulnerabilities — continue to grow.

Talk to the heads of the several CI components today and you will learn that no one of them knows what the other has to bring to the table. Why does this matter? Because it is impossible to match means to ends if you do not know what means are at your disposal – much less to assess where or how far you have fallen short.

You will also learn that, twenty years after the creation of the national CI office, no one has a common operating picture of what the United States is doing against foreign intelligence targets. In July, the head of the British Secret Intelligence Service reported that, subsequent to Russia's invasion of Ukraine, European governments had expelled over 400 Russian intelligence officers serving under diplomatic cover – adding that he hoped that others will consider turning on Putin ("Our door is always open"). So who is keeping book on how many cases the FBI has today on the Russian target (never mind the specifics of who/what/when/where, or the possibilities for operational exploitation)? The same holds true for U.S. efforts to identify, assess, neutralize or exploit the intelligence activities of the Chinese, the Iranians, and other adversaries working actively against us.

It is yet another step to be able to answer the question, "Are we winning or losing?"

Our inability to answer that question should make all of us very uncomfortable. This Committee is very familiar with the relentless Chinese and other collection networks directed against U.S. business and industry and commercial wealth. Cyber-attacks against our critical infrastructures and sensitive databases have grown so aggressive that they have been assigned as part of the defensive mission of a unified combatant command (USCYBERCOM) and a dedicated agency (CISA) at the Homeland Security Department. Indeed, these threats, it is often said, require a "whole of government" response, including specialized analytic and operational contributions that only counterintelligence can make.

What gets far less attention are the hostile penetrations and foreign deception operations that have grown far bolder and deeper than the resources we have available to counter them, putting lives and treasure and U.S. supreme national interests at risk. A few examples:

> ***China:*** According to media reports,[5] significant U.S. intelligence operations in China have been compromised, which, if true, raise many questions, which this Committee may wish to explore in closed session. For example, how were these operations discovered? How long were they being observed … and played back against us? How many other losses have

yet to come to light? What more do the Chinese know about U.S. intelligence operations? And how are they using those insights to hide what they are doing or otherwise deceive us? Simply put, if you thought we had good intelligence on the Chinese, think again.

How all this might have happened appears to be a matter of dispute. What is not in dispute is how thoroughly devastating such losses could have been and continue to be to U.S. intelligence – and all who depend on that intelligence to make life and death decisions.

Russia: Human intelligence is still Russia's forte. For the Russian intelligence services, America has always been deemed the "main enemy:" the outcome of the Cold War has only reinforced their focus, not changed it. By contrast, the West's intelligence efforts against Russian targets were sharply reduced as the U.S. waged a global war on radical Islam – and also because we thought a post-Cold War Russia would no longer be counted among our adversaries. Then Putin invaded Ukraine. And now we're playing catch-up.

Major Soviet/Russian espionage cases (i.e., penetrations into the U.S. government, run directly or through proxies) numbered 16 in the 1980s, 10 in the 1990s, one in 2001 ... and then nothing, until a former Army Special Forces officer was arrested last year for selling the Russians information about weapons and troop deployments. And no, the sharp decline in arrests and prosecutions is not good news.

While the numbers have fluctuated over time, there are well over 60 Russian intelligence officers stationed in the United States today (not counting illegals or those here under non-official cover). Their highest priority? To recruit assets inside the U.S. intelligence community. Putin is a former KGB/FSB head. He's grading their performance. How likely is it that they're just sitting around with nothing to show for it? Yet we found no penetrations for two decades. If you do the math, it's not reassuring.

Cuba: "Havana syndrome" - unexplained and sudden brain injuries affecting dozens of American personnel – may or may not have involved the hand of the Cubans when first reported there in 2016. But at a minimum it poses the troubling question of why we don't have deeper insights into the secret operations of the Cuban government, especially ones that put Americans at risk? In all likelihood, U.S. intelligence insights into Cuba have been thin to nonexistent for decades, thanks to the stunningly successful deception and denial campaigns of Cuban intelligence operating under our noses here in the United States. You can't get an accurate read on foreign threats if your sources are corrupt, your agents doubled back against you, and your intelligence collection apparatus blind and deaf and dumb - but you don't know it.

Recent press reports[6] suggest that troubling compromises continue to plague U.S. intelligence, putting uncounted lives at risk, clouding the integrity of intelligence reporting, and bringing deep poignancy to the question, now what?

One Team, One Plan, One Goal – or not?

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("WMD Commission"), chartered to review intelligence failures in the aftermath of the Iraq War, devoted substantial attention to U.S. counterintelligence. In

welcoming the President's 2005 *National Counterintelligence Strategy*, they cautioned that a strategy alone is not enough:

> Our counterintelligence philosophy and practices need dramatic change, starting with ***centralizing counterintelligence leadership***, ***bringing order to bureaucratic disarray***, and ***taking our counterintelligence fight overseas*** to adversaries currently safe from scrutiny.[7]

I believe the principal obstacle to effecting this change was then and remains today the lack of consensus on the job that the national office and the CI components together were being asked to accomplish.

Despite the WMD Commission's indictments and calls for change, despite the passage of the *Counterintelligence Enhancement Act* and the searching critique of CI-21, there were then and are still many CI professionals in intelligence and law enforcement who believe the United States is already doing all that can be done against the foreign intelligence threat. That self-evaluation might well be accurate in the context of traditional CI responsibilities with very limited budgets -- but it misses the point behind the strategic CI mission.

The 2002 reform legislation charges U.S. counterintelligence with executing a new mission that cannot be performed by independent entities acting without central direction or strategic coherence. The intent was not to impose a new layer of bureaucracy, or peel away authority or responsibility from the several operational organs, but to assign additional duties to each of them to meet strategic CI objectives. The objective was to integrate the diverse capabilities of the U.S. CI enterprise at home and abroad to go on the offense against hostile intelligence threats directed against the United States.

To be sure, foreign intelligence personnel are already at or near the top of the DO targeting list. (Clandestine HUMINT, of course, is not the only collection means of value against foreign intelligence operations.) But it is one thing to check the box for recruitment opportunities, and quite another to have a top down, strategically orchestrated effort to disrupt and degrade the operations of a foreign intelligence service. Moreover, while there is no question that the orientation and work ethic of individual FBI agents and other CI professionals are very pro-active when it comes to working individual cases, there is a vast difference between the personal initiative exhibited by a law enforcement officer or a CIA station and the coordinated strategic initiative demanded of the Nation's lead executing agencies for CI.

The challenge remains how to pull together a strategic CI capability -- one team, one plan, one goal. To that end, CI professionals need to have a clear understanding what we are trying to achieve... of what they together are being asked to achieve. And here we have a problem.

Neither "strategic counterintelligence" nor a strategic CI program is defined in law, or anywhere else. The very concept of a national counterintelligence mission, different from what the operating arms are already doing, is new and untested. And CI leadership knows that objectives set forth in a national strategy one year can change in the next-- and have.

The President can issue strategies, the interagency can table implementation plans, the budget examiners can have their say, but at the end of the day it is what the operators actually do

against the adversary that will matter most. Without the discipline of a national program, CI management will continue to measure performance against the individual agency metrics for which they are accountable, as they must. But is that enough to counter the foreign intelligence threats directed against the United States?

Unique Roles/Responsibilities of Counterintelligence

A fundamental purpose behind creating a head of U.S. counterintelligence was to hold someone accountable to the President and the Oversight Committees for answering that question. In particular, does the federal government have the capabilities required to influence by deception, compromise by penetration, or disrupt by arrest or expulsion the threats posed to the United States by hostile intelligence services, their officer cadre, agents and proxies? That scorecard today may be very much in doubt.

By default, the field gets occupied by security or risk management practices on the one hand, and collection on the other, with far less attention or resources devoted to the operational responsibilities of U.S. counterintelligence. The two-way relationships with security and collection are intricate and absolutely essential – but there is a field of endeavor that is uniquely CI which is too often neglected because these other things have metrics and immediacy that are so much more familiar and demonstrable.

Indeed, the practical objectives of CI and security are not always in concert, "one of the classic conflicts of secret operations."[8] It is the duty to engage the adversary (an anathema to security, which wants to keep the adversary as far away as possible), and the duty to take action to exploit or disrupt them (which is at odds with collection), that form the heart and soul of counterintelligence. While there are defensive aspects to CI tradecraft, the imperative to penetrate and control the adversary service is what the CI mission is all about.

This Committee called attention to the importance of the security/CI distinction in its 1986 report, *Meeting the Espionage Challenge*:

> An effective response to the foreign intelligence threat requires a combination of counterintelligence and security measures. The Committee believes it is important to distinguish between counterintelligence efforts and security programs, while ensuring that both are part of a national policy framework that takes account of all aspects of the threat.[9]

In practice and by executive order, counterintelligence is closely related to, but distinct from, the security disciplines:

- Counterintelligence authorities and responsibilities are assigned by Executive Order 12333. Those 17 entities – not every potential foreign intelligence target – make up the CI enterprise.
- Security by contrast is a "command function" (in military terms), meaning that the head of each department/agency/office/post/private enterprise is responsible for the guards, gates, locks, personnel, firewalls, *etc.,* protecting their assets and operations against foreign intelligence threats as well as other compromise, theft or loss.

- As this Committee explained, "counterintelligence measures deal directly with foreign intelligence service activities, while security programs are the indirect defensive actions that minimize vulnerabilities."[10]
- The CI mission includes providing threat assessments to federal departments and agencies, as well as outreach to the private sector; but their respective security offices are responsible for developing and implementing the plans and programs they deem necessary to reduce their vulnerabilities. In practice, there are very close working relationships between security and CI officials, with especially well-developed protocols for handling insider threat issues.
- Other government entities such as the Committee on Foreign Investment in the United States also need insights into foreign intelligence activities (*e.g.,* supply chain exploitations, front companies) in the course of their work; again, they are consumers of CI analytic products but not part of the CI enterprise.

Why do these distinctions matter?

Under DNI James Clapper, the Office of the NCIX was rebranded the National Counterintelligence and Security Center (NCSC) – one of four such centers within the Office of the DNI. While co-mingling the two may seem benign, in practice that model has a long-standing track record of drawing time, attention and budgets away from the very difficult business of identifying, assessing, disrupting and exploiting foreign intelligence operations. By its nature, security has an unbounded appetite for dollars and attention. It is the here and now versus the longer-term, strategic needs of counterintelligence. And the here and now always gets priority.

Counterintelligence may be the most manpower-intensive mission of all the national security disciplines, short of war. Espionage investigations, in particular, require the investment of years of detailed analysis, surveillance, translations, asset development, intelligence collection and other operations. While just one well-placed spy can exact a tremendous amount of damage, the hunt to find him or her typically involves a huge amount of work often around the clock by teams of people with nothing to show for it for years at a time, if ever.

That workload did not diminish when the Cold War came to an end. The freer movement of people and goods across borders also meant more freedom of movement for adversary intelligence services targeting the United States. Even so, after the "peace dividend" cuts of the mid-1990s, followed by the sweeping, overnight reprogramming of personnel from CI to counterterrorism after the terrible events of 9/11, CI resources at the FBI dropped 50% from Cold War levels, where they have hovered ever since.[11]

Today, the FBI must cover more than 800 trained and state-sponsored foreign intelligence officers embedded within a standing foreign diplomatic community of more than 30,000, which provides operational cover-for-action from more than 800 buildings in more than 30 American cities, each of which enjoys diplomatic immunity. Of the foreign intelligence services highest on the annual National Threat Identification and Priority Assessment, U.S. counterintelligence has resources to cover fully less than 10% of their personnel residing in or transiting the United

States. And according to Director Wray, the FBI is opening a new China-related counterintelligence investigation every 10 to 12 hours (not to mention all the others).

By any measure, U.S. counterintelligence resources are stretched very, very thin.

As national leadership looks increasingly to our CI agencies to shoulder the security mission, it may well be exacerbating the problem, as scarce CI resources are diverted to other purposes – giving adversary intelligence services a freer playing field in which to operate. Paradoxically, if more robust security is bought at the expense of the U.S. government's ability to counter hostile intelligence operations, then America's national security secrets, critical infrastructure and technologies, and proprietary information will end up more at risk.

With the best of intentions, our CI leadership may be making matters worse by broadening its use of the term "CI community" to include government departments and agencies, along with private industry and academy, who are responsible for their own security plans and programs and thus need to be aware of foreign intelligence threats. Here, the FBI has taken the lead in standing up joint "CI" task forces, engaging interagency partners and reaching out to community leaders, in all 56 field offices, plus a National Counterintelligence Task Force to consolidate and build upon those efforts. But security is not CI.

In London during the Blitz, air raid sirens warned the population of approaching enemy bombers so they could take cover, while anti-aircraft artillery and fighter interceptor squadrons were deployed to take out the bombers. Protection is vital – and so is offense. Similarly, while the security mission is vital, so is countering hostile intelligence threats. It's up to counterintelligence to find and take out those allegorical "bombers" – preferably long before they reach their targets.

Yes, strengthen security, educate the public, pursue legal remedies, engage social media platforms to block dangerous content, counter disinformation with the truth. These are all essential protective measures against foreign intelligence operations directed against us. But they are not enough. They will never be enough.

We are ceding the initiative to our adversaries. That has to stop. So whose job is that?

A Charter for the NCIX/NCSC?

One of the strengths of a democracy that holds Presidential elections every four years is the infusion of new ideas. Institutional memories and professional cadres are of unquestionable value to any government organization. But so is the opportunity for new leadership to bring fresh eyes, a new vision, and new energy.

The evolution of the NCIX, now the NCSC, is no exception. As I look back at the record of my time in office, and that of my four successors over the past four Administrations (with President Biden's head of counterintelligence, as of this writing, still to be named), I see different paths, different priorities, and different outcomes. In particular, the need to respond to broader national level concerns has commanded the time and attention of the office.

I came into the job when the country was at war, still suffering from the wounds of 9/11 and determined never to let anything like that happen again. The strategic offensive orientation of

the national CI mission, as captured in the 2005 National CI strategy, is in part a reflection of that determination. Cyberthreats would receive more prominent attention by the head of U.S. counterintelligence in years to come, as OPM data bases were raided by Chinese (and other) cyber ops, along with countless other sensitive government and private sector IT infrastructure, with the true extent of damage still unknown -- and growing.

And there is no question that compromises by insiders, especially the cases of Snowden and Manning, led to voluminous damage assessment work and the institutionalization of insider threat task forces and program metrics across the federal government, under the leadership of the national CI office.

The decision by DNI Jim Clapper to merge the security portfolio under the head of U.S. counterintelligence further expanded the Director's responsibilities. To date, the NCSC has compiled a solid record of accomplishment in outreach and public education, supporting interagency security efforts, and complementing the FBI's longstanding, close interactions with business, industry and academia.

By contrast, the imperative in creating the NCIX was to put someone in charge of U.S. counterintelligence, in order to bring strategic coherence to the enterprise. In 2016, we saw the first concerted effort by a foreign power to influence the course of a U.S. presidential election, which proved only a first wave of malign influence operations to come. In this fight, U.S. counterintelligence has specialized resources to bring to bear – and which, in my view, warrant the focused attention of the national CI office.

Unfortunately, two decades after its creation, there is no enduring agreed vision for what the NCIX/NCSC should be doing.

If the measure of effectiveness is how many awareness briefings have been provided to key industry leaders, how many background investigations have been processed, what new intrusion detection software has been promulgated, and how many agencies have met their insider threat program objectives, then I believe the record of the NCIX/NCSC will show important strides over the past 20 years.

But if the measure of effectiveness is how successful we have been in building a national-level, strategic capability to identify and disrupt hostile intelligence operations directed against the United States, then we need to give ourselves an "F."

Throughout history, America's counterintelligence professionals have made tremendous contributions to the security of our Nation. Thanks to their dedicated work, there is no reason to doubt that we are deriving about as much value as possible from the old business model of U.S. counterintelligence. But the sum of what our CI agencies do will not bring us a strategic offensive gain against foreign intelligence threats unless orchestrated to a common end.

This essential orchestration was to have been the new and force-multiplying job of the national head of U.S. counterintelligence.

If a goal is understood, then it should be possible to build an effective team to accomplish it; but without that shared vision, there is little prospect for unity or success. If I could go back in time and accomplish just one more thing before stepping down as the NCIX, it would be to draft

a charter for the organization -- not to constrain its ability to take on new tasks but to ensure that it does not lose sight of its unique core mission. I hope that a future Director/NCSC will pick up that pen, to set forth an agreed set of responsibilities, processes, and objectives of the national CI office – and its value added to U.S. counterintelligence.

Proposed amendments to CI Enhancement Act

The central judgment of the *Counterintelligence Enhancement Act* is clear. There is a national CI mission that is beyond the ability of any individual Agency to fulfill. This mission can only be accomplished by ensuring the integration and strategic direction of CI community operations and resources. The law places the responsibility for that coordination on the statutory head of U.S. counterintelligence. But responsibility without the means of carrying it out is illusory.

As this Committee reviews the U.S. CI landscape, and measures requirements against threat, I would invite your attention to two statutory changes which, in my opinion, are needed to clarify the original legislative intent behind the *Counterintelligence Enhancement Act of 2002*. First, defining in law the meaning of "strategic counterintelligence" would help advance much needed common understanding and unity of effort. Second, establishing a formal national CI program (with associated budgets, billets, and accountability) would lay the groundwork for the single most important new capability the United States must have in defeating hostile intelligence threats directed against us. Below are some ideas, for your consideration:

Definition of strategic counterintelligence: ***The term "strategic counterintelligence" means the direction and integration of counterintelligence activities to compromise or disrupt the ability of foreign intelligence services to harm U.S. national security interests at home or globally.***

Statutory Strategic Counterintelligence Program: ***U.S. national counterintelligence shall develop options to degrade the ability of [nation state] to project force or prosecute national objectives, establish or maintain hostile control, or conduct operations or collect intelligence against U.S. interests globally, by means of their intelligence activities.***

Illustrative Report language: It is the intent of Congress that the D/NCSC, as head of U.S. counterintelligence, shall serve as the director of the strategic CI program. Subject to the guidance of the DNI, the D/NCSC shall be assigned the resources, authority and responsibility to cause the Departments and agencies of the Executive Branch, charged by Executive Order and law to execute CI activities, to allocate and commit sufficient CI resources to the long-term execution of the strategic counterintelligence mission and the National Counterintelligence Strategy, and the prosecution of high value CI targets. In carrying out this section, the DNI (D/NCSC) shall establish a pilot strategic CI program, and report back with an implementation plan covering *inter alia*

a. A policy framework to support the designation of High Value CI Targets, where such analysis determines that the foreign intelligence activities pose a serious risk to national assets or programs, or implicates the resources, equities, or operations of more than one Department, agency, or USG element.
b. Resource requirements to maintain a High Value Counterintelligence Targeting Center, the purpose of which is to provide global and persistent monitoring, collection, and

analysis of the movement, intentions, associations, and communications of designated foreign intelligence cadre.

c. Strategic operational planning team or teams to identify intelligence gaps, collection requirements, and options for degrading High Value CI Targets as assigned. This includes deep-dive strategic analyses of adversary services plans, intentions, capabilities, and vulnerabilities to enable operations to neutralize them, marshalling the resources of the operational CI entities to a common end.
d. Tasking protocols for distributed execution by the CI operational elements within their spheres of responsibility, and associated budget requirements.
e. Evaluation and accountability metrics for strategic CI program activities.

---

[1] As then SSCI Chairman Bob Graham explained, "At the urging of our committee, the President created the NCIX in 2001 to provide the U.S. Government in the counterintelligence area with (1) strong, policy-driven leadership; (2) new and enhanced counterintelligence capabilities; and (3) coherent program, strategies and cooperative approaches. The committee's oversight of this fledging effort revealed problems, however, that [this Act] is designed to remedy. By establishing the NCIX in statute and placing it in the Executive Office of the President, with oversight by the intelligence committees, the committee believes that the NCIX leadership problems, resource constraints and, overall, lack of sufficient status and visibility within the Government, will be remedied." Daniel Robert Graham (FL), "Intelligence Authorization Act for Fiscal Year 2003" *Congressional Record,* Vol. 148: September 25, 2002, p S9352**.** The NCIX office was subsequently moved under the Director of National Intelligence and renamed.

[2] "Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities." 50 USC 3003(3)

[3] Of note, CIA officer Aldrich Ames and his Soviet/Russian handlers had benefited from those seams for 9 years, FBI special agent Robert Hanssen for 21, and DIA analyst Ana Montes – Cuba's star asset – for 17. (Montes, serving a 25-year prison sentence, is scheduled for release next year.) Waiting in the wings was Katrina Leung, whose prosecution as an 18-year Chinese double-agent was truncated by management and oversight failings documented in the follow-up Justice Department Office of the Inspector General report https://oig.justice.gov/sites/default/files/archive/special/s0605/index.htm Of course, there would be more to come.

[4] James M. Olson, "The Ten Commandments of Counterintelligence," *Studies in Intelligence*, Fall-Winter 2001, CIA Center for the Study of Intelligence, Washington DC

[5] "Killing C.I.A. Informants, China Crippled U.S. Spying Operations". *The New York Times*, May 20, 2017.

[6] "Captured, Killed or Compromised: C.I.A. Admits to Losing Dozens of Informants" *The New York Times, October 5, 2021*

[7] *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Report to the President of the United States, March 31, 2005, p485; emphasis added.

[8] Christopher Felix, *A Short Course in the Secret War*, 4th ed. (Lanham, Maryland: Madison Books, 2001), 126

[9] *Meeting The Espionage Challenge: A Review of United States Counterintelligence and Security Programs,* Report of the Select Committee on Intelligence, United States Senate (99th Congress 2nd Session) October 3, 1986, p38.

[10] Ibid

[11] To add to the problem, in 2006 the DNI tasked this diminished CI workforce, subject to law and the protection of civil liberties, to take on a whole new job: to collect intelligence on the broad sweep of national intelligence priority targets -- with no new resources assigned for that purpose. That tasking – as another duty as assigned – still stands.

STATEMENT OF KEVIN GAMACHE, PhD, ASSOCIATE VICE CHANCELLOR AND CHIEF RESEARCH SECURITY OFFICER, TEXAS A&M UNIVERSITY SYSTEM

Dr. GAMACHE. Chairman Warner, Vice Chairman Rubio, Senator Cornyn, and members of the committee. Thanks for allowing me the opportunity to testify before you today. I'm the Chief Research Security Officer for the Texas A&M University System and come today to discuss the unique challenges universities face in protecting cutting-edge U.S. research. With four decades protecting our national security, first as an Air Force nuclear operations and maintenance officer, for 14 years in my current position, and as a faculty member at Texas A&M, I'm glad to have the opportunity to bring these perspectives to this critical issue.

One of the primary roles universities play is the free and open generation and dissemination of knowledge. The collaborative nature of the U.S. research enterprise is a prime source of discovery and innovation. International collaboration is crucial to scientific advancement and the success of U.S. research institutions. American universities are a magnet for students and researchers worldwide to join forces to advance science and solve our most pressing problems. Unfortunately, we're not playing on a level field. Our technological leadership is under siege from countries like Russia, China, Iran, and others whose rules for research integrity differ from ours.

I'd like to highlight a few organizational and process changes we've implemented to address this significant threat. A&M Chancellor John Sharp established the Research Security Office at the system level in 2016 to provide program management and oversight of sensitive research across the 19 A&M System members.

We require mandatory disclosure of all foreign collaborations and approval of foreign travel.

We conduct continuous network monitoring using techniques explicitly focused on identifying malign foreign actors.

We updated our conflict of interest and commitment policies and established processes for reviewing and approving collaborations and agreements.

We established a secure computing enclave that is available system-wide to protect system federally-funded research.

Understanding our collaborators and their funders is the most critical aspect of our research security program. It is equally important to know if a foreign government nexus exists and the risk it poses to the institution.

We must also understand whether these risks can be mitigated or must be eliminated. We use a robust, open-source, risk-based due diligence process to review visiting scholars and postdoctoral researchers to answer these questions. You may have heard it said: we can't arrest our way out of this problem. We agree and have developed strong relationships with the FBI, DCSA, and other IC members to address issues promptly.

Federal-level opportunities to significantly impact the problem also exist. A national research security center of excellence in academia—working with the FBI, DCSA, and other agencies to coordinate the flow of counterintelligence information between academia,

law enforcement, and the Intelligence Community—would enhance efficiency and effectiveness.

Secondly, our adversaries would be less effective if U.S. faculty and students were resourced more fully through enhanced federal research funding. Top international scholars in our universities enhance innovation and knowledge but also prevent risks. Partnering with federal agencies to mitigate existing and emerging threats, educate our researchers, and provide clear avenues to address security concerns are crucial. Doing so will allow the U.S. academy to continue producing game-changing research and a skilled workforce and ensure U.S. technological and economic superiority.

Thank you for the opportunity to testify. I look forward to your questions.

Chairman WARNER. Thank you.

Mr. Sheldon.

[The prepared statement of Dr. Gamache follows:]

Dr. Kevin R. Gamache
Associate Vice Chancellor and Chief Research Security Officer
The Texas A&M University System

"Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center"
U.S. Senate Select Committee on Intelligence

Wednesday, September 21, 2022

About The Texas A&M University System

Chairman Warner, Vice Chairman Rubio, Senator Cornyn, and Members of the Committee thank you for the opportunity to testify before you today.

I come before you this afternoon as the Associate Vice Chancellor and Chief Research Security Officer of The Texas A&M University System to discuss the unique challenges of protecting our Nation's cutting-edge technology and maintaining our national security in the free and open environment of academia.

The Texas A&M University System is one of the most extensive systems of higher education in the Nation, with an annual budget of $7.2 billion. Through a statewide network of 11 universities and eight state agencies, the Texas A&M System educates more than 152,000 students. It makes more than 24 million additional educational contacts each year through service and outreach programs. System-wide research and development expenditures exceed $1 billion and are drivers of our state's economy.

The A&M System has been a member of the National Industrial Security Program (NISP) since 1974. As a NISP participant, the A&M System is a cleared defense contractor just like Lockheed Martin, General Dynamics, or the more than 12,000 other NISP participants upon whom our national security depends. The A&M System has been granted Facility Clearances by the Department of Defense and Department of Energy, and we currently conduct classified research for both organizations from our facilities at the flagship campus in College Station.

The A&M System's security program has amassed a record of seven straight SUPERIOR ratings during annual Security Vulnerability Assessments conducted by the Defense Counterintelligence and Security Agency (DCSA). DCSA recognized the A&M System in 2015 and 2020 with the Colonel James S. Cogswell Outstanding Industrial Security Achievement Award as one of 40 from more than 12,000 defense contractors subject to recurring security assessments. The award recognizes those security programs that far exceed basic NISP requirements and provide leadership to other cleared facilities in establishing best practices while maintaining the highest standards for security. DCSA also recognized the A&M System with their 2017 and 2019 Awards for Excellence in Counterintelligence, given to those contractors and universities that best demonstrate the ability to stop foreign theft of US defense and national security technology.

Addressing the Threat

One of the primary roles of academic institutions is the free and open generation and dissemination of knowledge. Known for its open and collaborative nature, the US research enterprise provides the foundation for a diverse and driven workforce, fostering discovery and innovation. International collaboration is crucial to scientific advancement and the success of research institutions in the United States.

American universities have become a magnet for students and researchers worldwide to join forces in solving our nation's most pressing problems and promoting scientific advancement. Unfortunately, we are not playing on a level playing field. Our technological leadership is under siege from countries like Russia, China, Iran, and others whose rules for information sharing and research integrity differ from ours. These countries are extracting intellectual capital, cutting-edge data, and technical expertise at an unprecedented rate and putting our technological leadership at risk. Academic sector entities must work closely with our federal partners to protect information and research with national security implications. To be most effective, integration and information sharing between the research security community and the U.S. counterintelligence enterprise must be seamless.

Acknowledging this risk, A&M System Chancellor John Sharp established the Research Security Office (RSO) at the System level in 2016 to provide program management and oversight of all classified research, controlled unclassified programs, and export-controlled research across the 19 A&M System members. The RSO manages the A&M System's relationship with DCSA and members of the Intelligence Community that conduct business on our various campuses. The RSO provides a "one-stop" office for A&M System members to visit with security-related questions and issues. The RSO is also responsible for assisting with the vetting of visiting scholars and ensuring compliance with federal regulations on information and data security.

Understanding our collaborators is one of the most important aspects of any research security program. With whom are we collaborating? Who is funding those collaborators? Is there a foreign government nexus? What is the risk to the institution? Is there a reputational risk? Can these risks be mitigated? To answer these questions, the RSO has established a robust open-source due diligence program through which we review all visiting scholars and post-doctoral researchers from countries of concern, all personnel engaging in our work with Army Futures Command, the University Consortium for Applied Hypersonics, and our national laboratory efforts, and others based on risk.

We require the mandatory disclosure of all foreign collaborations and approval of foreign travel. We conduct continuous network monitoring and have included keywords and signatures in our data loss prevention system explicitly focused on identifying malign foreign influence in our research enterprise. We have updated our conflict of interest and conflict of commitment policies and have established processes for reviewing and approving foreign collaborations and agreements.

We have established a NIST-800-171 compliant secure computing enclave that is available to all members of the A&M System to protect sensitive research funded by the federal government. The

secure computing enclave allows us to monitor the flow of information down to the project level. It precludes anyone who might achieve unauthorized access to our secure computing enclave from gaining access to more than a single research effort.

Underpinning all this work is our robust relationship with our federal partners, including the Federal Bureau of Investigation (FBI), DCSA, Department of Justice, and other members of the Intelligence Community. FBI Director Wray noted, "we can't arrest our way out of this problem." Collaborations between academia and the Federal government are critical to addressing these threats. The RSO serves as the single point of contact for the A&M System with our Federal partners. I engage with our FBI and DCSA partners daily to facilitate information sharing and joint operations.

Key to our engagement with our federal partners has been the establishment of the Academic Security and Counter Exploitation (ASCE) working group, an association of university research professionals and their federal counterparts, which exists to leverage the expertise of universities that have demonstrated excellence in research security programs to help address the threat foreign adversaries pose to U.S. academic institutions. The ASCE Executive Committee includes representatives from the FBI, DOD, State Department, and Commerce Department and meets bi-weekly to discuss threats to research security and mechanisms to combat them. The group works collaboratively to develop and share information on best practices for a successful research security program.

We established the first Academic Security and Counter Exploitation Training Seminar in 2015 to provide a forum for those academic institutions participating in the NISP to benchmark and share best practices from their respective programs. The conference has grown since that first year to include the broader academic community and increased federal engagement from the FBI, DOJ, DOD, NSF, NIH, Office of the Director of National Intelligence, and Office of Science and Technology Policy. We were honored to have Chairman Warner and Senator Cornyn join the conference in 2021 to talk about the threat and the work you're doing here in Congress. We're well on our way in planning for next year's conference, which will be held in College Station from March 6-10, 2023. This year's seminar will have an international component for the first time resulting from our partnership with the Department of State.

While the Academic Security and Counter Exploitation Training Seminar provides an opportunity for academic security professionals to come together physically once a year, we have also developed ongoing platforms for virtual collaboration. We created a listserv for security professionals in academia to seek advice, benchmark, and share best practices daily. The listserv currently has over 200 member universities and remains extremely active. We also established the Academic Counter Exploitation (ACE) Program as a secure portal on the DHS's Homeland Security Information Network to allow academic institutions to share threat information unique to academia. We also share a weekly ASCE Open-Source Media Summary as another mechanism to share information with academia. We are pleased to reach over 3000 readers each week across academia, the private sector, and the Federal government, including from Capitol Hill.

Recommendations

Academia has come a long way in understanding, accepting, and addressing the research security threat over the past five years. The danger facing university professors, students, and institutions from malign foreign actors and foreign intelligence is widely understood and accepted today. Still, work remains to improve the state of security and transparency across the research enterprise to allow us to continue to operate in an open and collaborative environment on the international stage. National Security Presidential Memorandum-33 (NSPM-33) will help in these efforts by setting forth the actions required by research institutions, including academia, to mitigate risks and enhance the protection of the US research enterprise.

Universities seeking to implement effective research security programs should consider an approach that puts several organizational, process, policy, training, and technology solutions in place. These solutions should focus on mitigating the risks to the research enterprise while protecting those characteristics that make the US higher education system the most productive and prolific worldwide research generator. The institution should integrate research security functions into every level of the organization. Institutional leaders should champion research security and integrity as integral to the overall success of the research enterprise.

Implementing an effective research security program can significantly enhance the security of an institution's facilities and intellectual capital. Research personnel must be aware of existing risks, be able to implement countermeasures when appropriate, and be observant of nontraditional collection activities directed at their institution to be effective. This outcome is possible only if all institution members know the range of threats to the research enterprise and actively support the risk assessment and management program.

Research security countermeasures take several forms, including process solutions, policy solutions, and technology solutions. Process solutions include vetting visiting scholars, monitoring computer networks for illicit exfiltration of data, incorporating data-loss prevention systems, and establishing robust risk-management and risk reporting frameworks. The RSO should integrate processes for securing the research enterprise into every aspect of university operations, including human resources, awareness and training, information technology, international travel, and business administration.

Conflict of commitment, financial conflict of interest, external employment, and international travel policies have important research security implications. Establishing clear, enforceable expectations in these areas through well-thought-out organizational policy is critical to an effective risk- management program.

Incorporating technical solutions, such as secure computing enclaves that meet federal requirements for information protection, into risk-management processes can provide a solid foundation for securing data while minimizing the burden on researchers. We were pleased to see the inclusion of a regional secure computing enclave pilot program in the CHIPS and Science Act (P.L. 117-80). This pilot would assist universities conducting federally funded research in meeting security requirements, such as NIST-800-171. The requirement to meet this standard exists regardless of the size of the university or the size of the research award. Yet, compliance can be

costly. The regional enclaves authorized in this bill would provide a secure network on which universities of all sizes could store their sensitive research. It would help universities better monitor traffic on their systems and enhance the protection of federally funded research from foreign theft. We look forward to working with the National Science Foundation as they implement this provision.

Just as there is a disparity between larger research institutions and smaller regional universities in their ability to protect sensitive information effectively, the capabilities of academic institutions to conduct effective due diligence in vetting visiting scholars vary widely. This is another area where the research security community could benefit significantly from sharing resources. Larger research institutions could serve as regional hubs that smaller universities could rely on for assistance and resources in vetting visiting scholars. These regional hubs would serve as clearinghouses for federal-level coordination with the counterintelligence community.

Finally, there is a need for a National Center of Excellence (COE) for Research Security within the academic community. This COE could be a focal point for developing awareness and training material tailored to academia. It could provide training to research security offices on practical techniques for vetting visiting scholars, among other topics. It could also offer advice and assistance to universities in establishing and maintaining effective research security programs. This National Center of Excellence for Research Security could build upon the work that groups like the Academic Security & Counter Exploitation Program have already begun.

Conclusion

The excellence of the US research enterprise is inseparable from its commitments to openness and academic independence, institutional autonomy, and discretion to operate in a globalized world. However, these qualities also engender vulnerabilities to national and economic security in a climate of sharpening strategic competition. Rest assured, our adversaries will not rest on their laurels and will attempt to adapt to our efforts. We in academia must remain vigilant to meet the threat and protect the intellectual property that makes our nation the most prosperous in the world.

While the most effective way to address this challenge is for the academic community to take the lead in establishing policies, procedures, and protocols to secure the research enterprise, this is not a fight we can win on our own. The U.S. Government, including NCSC and other members of the Intelligence Community, play critical roles in notifying, supporting, or defending academic entities from foreign intelligence attack, penetration, and manipulation. Our collective success is dependent upon the effective partnership working toward common goals. The Texas A&M University System takes these threats seriously and looks forward to working with you and our partners in the Federal interagency, academia, and the private sector to address them.

STATEMENT OF ROBERT SHELDON, DIRECTOR, PUBLIC POLICY & STRATEGY, CROWDSTRIKE

Mr. SHELDON. Chairman Warner, Vice Chairman Rubio, Members of the Committee, thank you for the opportunity to testify today.

Innovation is an essential theme of the American story. While the private sector is not the sole source of innovation in the country, it plays the leading role in making new innovations accessible to everyone. The private sector is incredibly diverse. When explaining CrowdStrike perspectives to the policy community, I mentioned that we protect 15 of the top 20 U.S. banks and a significant and growing portion of the U.S. "dot gov" domain. But given the nature of the hearing today, I also want to emphasize that we protect small organizations, from family-owned farms to cutting-edge startups. Cyberthreats have devastating consequences for families, communities, and the economy. In the aggregate, these consequences extend to national security.

I'm honored to share some insights from our work across government and industry and identify some areas where we, as a nation, can strengthen cybersecurity outcomes.

Today, the private sector faces a punishing array of cyber threats. CrowdStrike research published this month identified campaigns targeting 37 distinct industries and a 50 percent increase in interactive intrusions over the past year. Regarding nation-states, China, Russia, Iran, and North Korea present the most potent threats. States utilize cyber means for espionage, theft, extortion, coercion, disruption, destruction, and subversion. I've provided more detail on these threats in my written testimony, but here I want to cite intellectual property theft and supply chain attacks as key concerns for national resilience.

Different segments of the private sector have different needs, constraints, and capacities to defend against cyberattacks. Organizations with cybersecurity mandates have proliferated in recent years, but victims still struggle to know who to contact for what types of issues. Sometimes lost is a fundamental reality of the cybersecurity landscape. When a private company is the victim of a cyberattack and it cannot remediate the issue independently, it must turn to a private sector incident response provider. There is no U.S. government agency that has the authorities and capabilities to provide end-to-end cybersecurity services from hunting to remediation at scale.

As you consider options to clarify and strengthen NCSC roles and missions, please consider two points.

First, in some cases, significant IC information can be shared without impacting sources and methods. Government disclosures this year regarding Russian plans and intentions for Ukraine, including warnings about specific disinformation themes and advisories about specific cyberthreats, were very well received by industry.

Second, NCSC should endeavor to operate at scale. This probably means a preference for leveraging existing government structures, like the Joint Cyber Defense Collaborative and commercial service providers with significant reach. During my time at CrowdStrike, some of the most impactful changes I've seen have involved the ad-

vent of groundbreaking managed threat-hunting services and broader managed security services.

These provide a reliable, consistently high degree of protection 24/7/365, and it's worth exploring opportunities to make such services more widely available. It's further worth considering additional programs or efforts to make available concrete cybersecurity services.

As a community, we should undertake a more serious conversation about expanding national incident response capacity. A program that retains scope providers in advance for use during significant cyber incidents could expand the cybersecurity workforce and strengthen national resilience.

Thank you again for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Sheldon follows:]

SENATE SELECT COMMITTEE ON INTELLIGENCE

Robert Sheldon
Director, Public Policy & Strategy
CrowdStrike

Testimony on Protecting American Innovation
Industry, Academia, and the National Counterintelligence and Security Center

September 21, 2022

Chairman Warner, Vice Chairman Rubio, Members of the Committee, thank you for the opportunity to testify today. Innovation is an essential theme of the American story, so much so that the Constitution even includes a clause intended to protect it.[1] While the private sector is not the sole source of innovation in the country, it plays the leading role in actualizing new innovations from everywhere. This includes bringing to market developments based on the aggregate work of government, nongovernmental, and academic and research institutions. When the best innovations can reach scale, all Americans stand to benefit, in addition to many others around the world.

The private sector is incredibly diverse. When explaining CrowdStrike perspectives to stakeholders in the policy community, I am proud to mention that we protect 15 of the top 20 U.S. Banks, 69 of the Fortune 100 companies, and a significant and growing portion of the U.S. ".gov." But given the nature of the hearing today, I also want to emphasize that we proudly protect organizations of all shapes and sizes. We protect small, family-owned agricultural enterprises. We protect advocacy organizations for persecuted ethnic minorities abroad. We protect important nodes in domestic manufacturing supply chains. And we protect small start-ups commercializing cutting-edge research and development (R&D).

Like markets themselves, threats to the private sector are dynamic. Threats like theft, extortion, harassment and coercion, destruction, and espionage date back centuries or millennia. Analog versions of these threats exist today, but the advent of the cyber domain has changed their scope, scale, and impact. Over the past two decades, industry has faced an increasing onslaught of cyber exploitation and attack. All too often, these threats have devastating consequences for families, communities, and the economy. Particularly in the aggregate, these consequences extend to national security.

This hearing, and the Committee report that catalyzed it, are particularly timely. The private sector today differs materially from previous decades and the threat environment evolves with each passing year. As underlying conditions change, it's appropriate to periodically evaluate the array of institutions meant to protect industry, the services they offer, and in turn the basic expectations policymakers might place on elements of industry. I'm honored to share some

[1] Article I Section 8, Clause 8 (informally called the "Patent and Copyright Clause").

insights from our work across government and industry and identify some areas where we as a nation can strengthen security outcomes.

Overview of the Threat Environment

Today, the private sector faces a diverse and high-volume array of cyber threats. CrowdStrike research published this month identified campaigns targeting 37 distinct industries and a 50% increase in interactive intrusions over last year.[2] Regarding nation-state threats specifically,[3] numerous countries have developed cyber operations capabilities and routinely target U.S. industry. China (PANDAS), Russia (BEARS), Iran (KITTENS), and North Korea (CHOLLIMAS) represent the most potent threats.[4] These include:

Espionage. Cyber threat actors persistently spy on private industry. In some instances, they seek to steal intellectual property, later providing it to state-owned entities or national champions. In other instances, espionage targets sensitive business information, which can be leveraged to manipulate markets (e.g., by subverting bidding processes), understand corporate plans or strategies, or otherwise gain an unfair competitive advantage.

Theft. Cyber threat actors sometimes directly steal resources, typically currency or digital assets. These attacks can be sophisticated, compromising significant banking or payments infrastructure, or unsophisticated, and target poorly-defended individual accounts. A common form of attack is Business Email Compromise (BEC), where threat actors impersonate executives, hack and alter payment data, create fake invoices, or otherwise persuade finance personnel to make unauthorized payments. While eCrime actors conduct these types of attacks, so too do some nation state actors seeking to raise funds for government or military endeavors.

Extortion and coercion. Many attacks seek to extort victims for funds or other concessions. This includes ransomware campaigns or leaking or threatening to leak hacked data. These attacks can halt or severely degrade business operations and adversely affect corporate brand and reputation. Attacks like social media account takeovers and web defacements are more commonly associated with "hacktivist" actors than nation-states, but these techniques can be used for coercive effects.

Disruption and destruction. Relatedly, hackers can disrupt or destroy Information Technology (IT) and/or Operational Technology (OT) environments with wiper campaigns (which erase data

---

[2] *See generally, Falcon OverWatch Threat Hunting Report*, CrowdStrike (Sept. 2022), https://www.crowdstrike.com/resources/reports/overwatch-threat-hunting-report/.

[3] CrowdStrike tracks actors according to motivation, and typically classifies them as nation-state actors, eCrime actors, and "hacktivist" actors. At the Committee's request, I've focused my remarks on nation-state actors, but will briefly describe eCrime overlaps and use of more traditionally 'hacktivist' themes or techniques.

[4] *See* George Kurtz, *Testimony on Cybersecurity and Supply Chain Threats*, Senate Select Committee on Intelligence (Feb. 23, 2021 at 3)(Quick overview of CrowdStrike's threat actor naming conventions), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf.

including potentially that required to make devices function) and encryption (e.g., ransomware or pseudo-ransomware).

Subversion. In some instances, companies are attacked or their infrastructure subverted simply to attack other public or private sector entities. These supply chain attacks can be extremely targeted, affecting a single or small handful of victims, or can effectuate compromise of thousands or tens of thousands of victims.

Adjacent threats. Three additional types of threats with a nexus to cybersecurity are worth mentioning here. First, under the guise of security, some countries have formal or informal code-review requirements, requirements to provide encryption or other security-related data, forced technology transfer requirements, and/or excessive "lawful access" requirements. These threats are a form of mandated vulnerability by coercion, and they are most acute in countries with weak or nonexistent rule of law. The People's Republic of China leads the field in these areas, but other countries are following suit. Second, insider threat attacks can be analog in nature, but aided or made more severe by cyber means. And third, misinformation and disinformation attacks can target industries or brands and negatively impact their business prospects. Beyond the cyber domain, threats to industry with national security implications include forced joint ventures and physical threats to travelers or foreign staff.

Available Resources

Different segments of the private sector, as well as individual entities, have different needs, constraints, and capacities to defend against and respond to cyber events or incidents. Public, private, and collaborative organizations with cybersecurity-related mandates have proliferated in recent years, but victims sometimes struggle to know who to contact for what types of issues or concerns. Confusion can be heightened during a crisis. Primary collaborative forums and resources include:

Department of Justice (DoJ)/Federal Bureau of Investigation (FBI). The FBI, as well as the National Cyber Investigative Joint Task Force (NCI-JTF), has important investigatory authorities and a mandate to lead in "threat response," according to roles outlined in Presidential Policy Directive (PPD)-41. This includes "identifying threat pursuit and disruption opportunities."[5]

Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA). DHS is charged with coordinating the "overall Federal effort to promote the security and resilience of the Nation's critical infrastructure."[6] DHS is also the lead organization for "asset response," which includes a variety of functions such as "assessing potential risks to the

[5] *See Presidential Policy Directive – United States Cyber Incident Coordination*, White House (July 26, 2016),https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[6] *See Presidential Policy Directive – Critical Infrastructure Security and Resilience*, White House (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[targeted] sector or region, including potential cascading effects," and related activities as described in PPD-41.[7] Increasingly, CISA looks to proactively coordinate with key industry players through the Joint Cyber Defense Collaborative (JCDC), of which CrowdStrike serves as one of the 9 founding "plankholder" members.

Sector Risk Management Agencies (SRMAs). These agencies serve as the regular federal interface for the collaboration and coordination with sector specific critical infrastructure entities, and at times advance new regulatory requirements and share information about threats to respective sectors, including cyber threats.

Sector Coordinating Councils (SCCs), and Information Sharing and Analysis Centers (ISACs)/Information Sharing and Analysis Organizations (ISAOs). These organizations exist to facilitate industry collaboration at the sector-level or for particular functions or events. Some companies participate in multiple such structures, and each operate somewhat differently according to stakeholder needs and expectations.

Intelligence structures. In recent years, intelligence organizations have sought to communicate risks and threats more publicly to alert wider audiences. With respect to cybersecurity, NCSC and its antecedents have highlighted foreign intelligence services as a key threat. The National Security Agency's (NSA) Cybersecurity Collaboration Center (CCC) seeks to coordinate with industry "to prevent and eradicate foreign cyber threats to National Security Systems (NSS), the Department of Defense, and the Defense Industrial Base (DIB)."[8]

Private sector. Sometimes lost in this array of partnership opportunities and mechanisms is a fundamental reality of the cybersecurity landscape. When a private company is the victim of a breach or cyberattack, and it cannot remediate the issue independently, it must turn to a private sector incident response (IR) provider. There is no U.S. government agency that has the authorities and capabilities to hunt for adversaries across a victim IT environment, eject them, identify and resolve the attack vector, and help maintain or restore the victim's operations.

Cybersecurity and Counterintelligence

Numerous government entities have realigned and reformed in recent years to support cyber missions. The Committee's report describes the establishment of the National Counterintelligence and Security Center (NCSC) in 2014[9] and covers existing cybersecurity mandates. More recently, the Central Intelligence Agency (CIA) created the Directorate for Digital Innovation (DDI) in 2015;[10] CISA was formally established in 2018;[11] NSA launched the

---

[7] These roles are also enumerated within PPD-41 and the National Incident Response Plan.
[8] *See generally NSA Cybersecurity Collaboration Center*, https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/.
[9] *See generally History of the National Counterintelligence and Security Center (NCSC)*, https://www.dni.gov/index.php/ncsc-who-we-are/ncsc-history.
[10] *See* Sean Lyngaas, *Inside the CIA's New Digital Directorate*, FCW (Oct. 1, 2015), https://fcw.com/security/2015/10/inside-the-cias-new-digital-directorate/207156/.
[11] *See generally, About CISA*, https://www.cisa.gov/about-cisa.

Cybersecurity Collaboration Center (CCC) in 2020;[12] and Office of the National Cyber Director (ONCD) was created in 2021[13]–all in an attempt to better address cyber threats.

As you consider options to clarify or strengthen NCSC roles and missions, consider a few key functions. First is raising awareness at a leadership level about threats. Because threats evolve and new executives are minted every day, this mission area must be a continuous function to maintain rather than a task to be completed.

Second, NCSC may be able to process and disclose industry-relevant insights from Intelligence Community (IC) information or assessments. The most actionable information would relate to new taskings for foreign intelligence services or developments in targeting practices. (Industry and academia do develop their own points of view on these issues, and in certain instances may develop higher-quality or more timely information than that possessed by the government.) But NCSC can contribute to stakeholders' understanding by adding additional insights where possible.

Perhaps some useful intelligence along these lines is classified. And perhaps some portions ought to remain classified in order to protect sensitive sources and methods. But disclosing some types of information does not inevitably compromise collection details. Notably, government disclosures this year regarding Russian plans and intentions for Ukraine, including warnings about specific disinformation themes and advisories about specific cyber threats, were well-received by industry. Based on this intelligence, many organizations did take proactive measures to harden defenses. Others would be better suited to characterize effects on IC activities from such disclosures, but these examples illustrate how to communicate sensitive threats clearly and openly.

Third, NCSC should endeavor to operate at scale. The private sector is enormous, and engagement efforts that are not either targeted extremely precisely or available to thousands of recipients will probably fail to make systemic impacts. This is another argument in favor of optimizing for making information–even sensitive information–widely available. Too often, conversations about cyber collaboration devolve into tactical plans for clearing more people or providing classified infrastructure to industry recipients. Aside from the costs and operational burdens associated with such proposals, they will not scale to protect most potential victims.

Seeking scale also means NCSC should feel comfortable–and probably prefer–leveraging intermediaries to broaden its impact. This might include existing government structures like JCDC. Or it might mean use of commercial service providers to distribute warnings to, or implement defenses for, their customers or stakeholder communities.[14] Where IC organizations

---

[12] *See NSA's Cybersecurity Collaboration Center Celebrates its First Year*, NSA (Dec. 22, 2021), https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2881886/nsas-cybersecurity-collaboration-center-celebrates-its-first-year/.

[13] *See generally Office of the National Cyber Director*, White House https://www.whitehouse.gov/oncd/.

[14] *See George Kurtz*, *Questions for the Record - Hearing on the Hack of U.S. Networks by a Foreign Adversary*, Senate Select Committee on Intelligence (Feb. 23, 2021 at 1-3)(How the private sector has

consume private sector threat intelligence, doing so in a shared services model with broad distribution entitlements can expand reach and assist the greatest number of stakeholders.

Elevating Defenses

The cybersecurity community, spanning public and private actors, is consistently engaged in efforts to strengthen cybersecurity and resilience. Informed observers agree that we must make further improvements. Several lines of effort are worth noting here:

Private sector developments. The cybersecurity industry moves quickly to address emerging threats, and sophisticated private sector entities quickly integrate new solutions. The most impactful security concepts and controls of recent years, like those mandated for federal use by E.O. 14028 (i.e, Endpoint Detection and Response (EDR) and adoption of Zero Trust Architectures, as well as comprehensive approaches to logging security-relevant information) were forged by the private sector in private sector settings.[15] Adoption is still uneven across industry, but is trending in the right direction.

During my time at CrowdStrike, some of the most impactful changes I've seen have involved the advent of groundbreaking managed threat hunting services and broader managed security services, including managed identity services. Increasingly, this has become an industry-wide trend that responds to customer preferences to engage professionals to provide a reliable, consistently-high degree of protection on a 24 hours per day, 7 days per week, 365 days per year basis. Some organizations use these capabilities to overlay or augment existing security teams, others free up capacity for existing staff to focus on security program maturity or conducting proactive risk mitigation activities. As with other efficiencies, organizations recognize that effective risk mitigation does not require doing everything 'in-house.'

Streamlining and enhancing government services. Large and sophisticated private sector entities are aware of and participate in multiple collaboration structures. Participation can be time-consuming, and discussions can cover a wide variety of topics, some of which are more appropriate for certain corporate roles than others (discussions may span topics relevant to Executive, Security Subject Matter Expert, Legal, Compliance, and other personas). At a certain point, the creation of new structures can create 'noise' and dilute participation potential, so government entities should be extremely clear about the value proposition of any new entities. Efforts to reduce or abstract away existing complexity would be helpful for small and medium sized enterprises in particular.

Subject to these constraints, it is worth considering additional government programs or efforts that make available concrete cybersecurity services, beyond consultation and collaboration, to

---

promoted practical information sharing), https://www.intelligence.senate.gov/sites/default/files/documents/qfr-gkurtz-022321.pdf.

[15] *See George Kurtz*, *Testimony on Cybersecurity and Supply Chain Threats*, Senate Select Committee on Intelligence (Feb. 23, 2021 at 3-5)(Extended discussion on emerging cybersecurity controls and practices), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf.

certain entities. As a community, we should undertake a more serious conversation about expanding national Incident Response (IR) capacity. IR demand is incredibly elastic, and IR supply is relatively fixed. Broad-based, concurrent cyberespionage campaigns in 2021 with thousands of victims did strain national capacity. The best practice for private entities is to have an IR retainer in place, so a skilled provider can offer assistance within a stipulated time frame, and under other terms outlined in a Service Level Agreement (SLA). A program that retained skilled providers in advance for use during significant cyber incidents could expand the cybersecurity workforce and strengthen national resilience. Eligibility for benefits under such a program would likely be based on need or vulnerability (e.g., for small businesses), and/or on criticality (e.g, entities with a national security nexus or critical infrastructure entities with systemic importance).

Incentives. Over the years, policymakers and industry groups have cited tax incentives, such as tax deductions or credits, as a possible driver for increased cybersecurity investment. To date, these proposals at the federal level have stalled out. But such mechanisms have proven effective in shaping behavior in other domains and are worth consideration here.

Government procurement can be a vehicle for innovation in the security space. The Federal government is a large consumer of cybersecurity services and does leverage acquisition requirements to drive cybersecurity outcomes. This, in turn, shapes the broader ecosystem. This is appropriate, but contracting officials must be careful not to create insurmountable barriers to the adoption of new and more innovative providers, nor continue to reward providers delivering consistent vulnerabilities into government networks. From the perspective of a new company offering a new type of product or service, overwrought or overly-prescriptive procurement guidelines can operate as a barrier. This can also reduce security in some cases.

Regulatory approaches. Over the past 20 years, policymakers and industry groups have struggled to come to terms with the optimal role for regulation to drive better cybersecurity outcomes. At this point, the key questions are familiar. *Given that some adversaries have the resources of a state behind them, can any regulation successfully prevent a breach? Given that government entities suffer breaches from time to time, can they credibly advance regulatory guidance? Past a certain point, do additional regulations become compliance exercises with deleterious effects on security? Will specific regulations stifle innovation surrounding better approaches to security?*

Perhaps we will not today resolve these questions to the satisfaction of the entire cybersecurity community. But a few points are clear. First, cybersecurity is a shared responsibility, and private entities should take reasonable steps to secure themselves and their data. Defining 'reasonable' can be a challenge, but regulations that adopt a principles-based approach are better designed to evolve more quickly than those that mandate specific controls, which can become obsolete in light of new threats. Second, clear and consistent incident response requirements can improve cyber incident response practices in private sector organizations. At present, the scope and particulars of new requirements to report certain incidents to CISA are not quite resolved, and the SEC is currently evaluating new requirements for listed companies, which could create an

entirely different reporting threshold framework. Although well-intended, too many simultaneous efforts could create gaps, overlaps, or confusion. At a minimum, we must pay special attention, and make adjustments if needed, to avoid these outcomes. It is both unreasonable and impractical to expect the government to solve every cybersecurity problem, but the government can play a unique role in incentivizing the adoption of best practices and technologies.

Conclusions

Thank you again for the opportunity to testify today. The cybersecurity industry and stakeholder community have made significant strides in recent years to defend against all manner of cyber threats, including those from nation-state actors. But we have more work to do, and we must work together to ensure we're surfacing practical solutions. These solutions must reach scale in order to meet the magnitude of the threat. And we must make special efforts to ensure that help reaches the small and medium sized enterprises that need it most.

I would like to conclude with a reminder that the problems I've described here affect not just the United States, but developed and developing nations around the world. At this point, it is already clear that success or failure in meeting these challenges will tell some part of the story of how nations will rise and fall in the 21st century. Thank you, and I look forward to your questions.

###

Chairman WARNER. I want to thank the panel for their presentations.

There will be a second vote at some point. We're going to work through that vote. And unlike our normal process where we do seniority at the gavel in our public hearings, we do straight seniority. So, we'll do five-minute rounds.

My first question is for the panel. And it's a two-part question. One of the things that this Committee took on after literally years of having almost weekly and sometimes biweekly briefs around the threats posed by the CCP was it seemed like we were existing in two parallel worlds. We were hearing all these threats and concerns, and yet, the economic message that was going around was the more we partner with China, the better. The more we bring China into the global world order, the more that we're going to have similar systems. Starting back in 2017, we, on a bipartisan basis, started going out—and I know you were involved in a number of these, and I want to thank all my colleagues who participated—and did a series of classified briefings for industry sector after industry sector. And the disconnect between what we were hearing in the intelligence briefings and what they were being told by Wall Street, or in terms of academic exchanges or academic freedom, was night and day.

And some of those were challenging sessions. Dr. Gamache, I'm glad to hear your comments about what you started doing 2019, but the number of universities that had no idea about, somehow, professors getting all-expense-paid trips to lecture in China and not thinking about even preconditions, like maybe you ought to not bring your laptop along, were pretty chilling.

We've done close to 20 of these. We did a number of them before COVID. Post-COVID, we've seen a great tick-up, and I want to thank academia for improving. And I think we have started to reach some ideas around consensus. Again, a lot of us on this Committee led the effort to try to put in place a cyber-incident reporting requirement.

But the question I have, and I'm going to break it into three categories:

Non-intel U.S. government and state government and local government entities; Academia; and private enterprises.

Assuming you got a continuum that at least in terms of government, where there maybe ought to be higher standards, are there standards? Legal, moral? What are the roles of informing those three entities about the threat? And should we just rely on best practices in terms of academic protections? Should we put in jeopardy federal funding? We have started on cyber incident reporting. I think there's a greater recognition. Obviously, well-regulated industries have standards, but cross-cutting standards we still lack.

I think I'll go down the list the same way we started. If you want to comment briefly on all three of those categories and whether there should be simply moral challenges, legal, or standard.

And I know Senator Cornyn, Senator Casey have got some legislation about investing, but let's take those three areas, legal, moral, and standard, as a setting in each of those three subsets.

Bill.

Mr. EVANINA. Thank you, Senator. A really difficult question. And I think that gets to the crux of where we are on—in today's battle in this gray area of—even from open research to private sector to our adversaries. I think we look at your question, I think Texas A&M should be commended for what they have done and what Dr. Gamache has done in the last few years in setting a standard with others in the academic community from a compliance perspective.

And I would proffer that they do more than 95 percent of the other academic institutions and research institutions do. And I think setting at least a minimum standard would be great from what the—using Texas A&M as a model. But I also proffered to you on the state, local, and federal government, and the non-Title 50s don't do anywhere near what Texas A&M does, specifically with their federal funding and subsidies that they give to research institutions.

So, I think there is a baseline to start with. And I would make it analogous to the idea of the Internet of Things. If we don't start with the baseline fundamental security apparatus, we're never going to get to a utopia state of having the right structural organization authorities. But understanding the problem is phase number one. And I thank or commend this Committee, yourself and Senator Rubio and Senator Burr and others for those road shows because they were influential to the people who drive our national economy, for making them understand the complexities on the global engagement and economic well-being in dealing with China.

The same time, their role and responsibility in protecting our Nation in what they do.

Chairman WARNER. Michelle.

Ms. VAN CLEAVE. Mr. Chairman, what you have described is no small challenge to business and industry to academia. I would offer that while the scale and magnitude of what we're facing today is staggering, it's not entirely new in the way the United States had to deal with threats to our business and industry.

And I recall being then in the Bush 41 White House, working in the Science Office for the President when the wall came down and everything changed. Globalization meant that there was more commerce and interaction and movement of people. And our immediate concern was, so we're going to find that the U.S. R&D and S&T base is now going to be raided all the more by foreign actors who are exfiltrating IT and technology, and everything's to their own benefit.

So, back then, I remember on my first interaction, working with the FBI, they were setting up, at the time, something called the National Security Threat List where they were trying to understand what things might be targeted by business and industry. Well, fast forward. And I think that we have a continuing need for providing awareness that the counterintelligence world gains the insights into what these foreign intelligence services are doing and how they're doing it against us, and foreign intelligence services and beyond using other instruments beyond their intelligence community to acquire and target our IT and our proprietary information.

And those relationships that the FBI has established, they're working very hard. They've created a national CI Task Force, and task forces within all of the 56 field offices, to build upon the relationships that they have with business and industry to try and do outreach with them. And I do think we need to be doing as much of that as possible.

But I would offer that, first, we have to have the insights. And first, we have to understand what the foreign intelligence services in other countries are doing against us. In order to have those insights, we're turning to our counterintelligence world—hard-core CI going out and learning how these services are operating against us so that we can better protect ourselves and stop them.

Chairman WARNER. Thank you. Dr. Gamache.

Dr. GAMACHE. I'd like to say that from what I see in academia, things have greatly changed over the last five years. The level of awareness, I think, is definitely heightened over what it was five years ago. But that's not good enough. You know, we've come a long way. The awareness level is greatly enhanced, but we've got a long way to go. I think NSPM–33 is a great start, but it's probably not enough in terms of providing direction and creating avenues for awareness that don't exist right now.

Helping academia understand how to address the threat once they become aware of it and having a structure to partner with, federal agencies—you know, right now, it's a pickup game. I think increasing the level of awareness in academia, providing guidance on how to address the threat, and then creating a structure to partner with federal agencies in a consistent manner is important.

Chairman WARNER. Thank you. Mr. Sheldon.

Mr. SHELDON. Thank you, Mr. Chairman.

Awareness of the threat is important. There are of course of people in town who frequently will remind people that there is a cyberthreat. It is very significant. People should do basic things like increase hygiene on their networks, do things that are best practices like use multifactor authentication. And that will only ever get us so far. I think that there's a couple of ways that we can incentivize organizations to move more quickly to provide defense for themselves. Those include some of the more regulatory options that we're exploring right now as a community. I think that this Committee was instrumental in starting off the conversation around incident reporting, and we'll see how that shapes out at CISA. But, certainly, there's a lot of good progress made toward that. That looks like it will be able to empower CISA to be able to make more assessments about how they can improve mitigations for particularly industries that are targeted within the same sector.

The other part of the conversation from our point of view is being able to start having more detailed plans for making resources more broadly available to the most vulnerable organizations, because for folks that are Fortune 500 companies, for example, very frequently, they have robust security programs. And they're doing what can be done to stop the threat that they're facing. But there's a lot of small- and medium-sized businesses that are being left behind for lack of resources. And the problem isn't exactly lack of awareness.

Thank you.

Chairman WARNER. Thank you. I'm sure we're going to come back and revisit. And second vote has started.

Senator Rubio.

Vice Chairman RUBIO. And I'm going to shorten my question.

So, I guess the first, Mr. Evanina, going back to your time in service, if you were to go back and sort of reanalyze some of the authorities and/or mission that you wish had been clearly delineated, what would those have been, given the new threat landscape that we've described here already?

Mr. EVANINA. Senator Rubio, looking back at the six-plus years I spent there, a lot of the success the NCSC had was predicated upon a few things:

Partnership with the other intelligence agencies and some of the non-Title 50 agencies in the spirit of trust;

Lack of duplicity, ensuring that we did not do the same type of analysis and operational work as any other agency and we were not operational.

But thirdly, I think the demand signal that we got from the private sector and others about what is the threat and how it's manifesting.

I think we look at the other agencies in that space, their job is operational OCONUS and CONUS. And NCSC took that ball and ran with the policy and strategy part of it. I think the hardship that you're talking about now would be, and to Michelle's point, the lack of clarity in the legislation, in the enhancement act, about legitimate authorities and roles.

I think that would be one thing. Starting all over again, a reunification of that act and what those roles, responsibilities are, it's beyond being the strategy policy organization.

Vice Chairman RUBIO. I think one of the hardest things to do today is to go to someone in public life or a public figure and say, these individuals that you think are your friend, they're your friends, these individuals that are business people, these individuals you know that are former politicians or claim to be journalists—are actually being sent here.

They may not even know it to sort of influence the things you're writing, saying, or repeating. The disinformation piece is really complicated because sometimes people think they're getting verifiable information. They think they have a scoop, or they just want to say something relevant. That's just not the way we think of foreign intelligence operating, especially if they're using multiple cutouts to get to that stage. And that's what we're going to be struggling with for some time.

Mr. Sheldon, on the challenge that I know with cyber in general, we often think about it as ransomware and things of that nature. But one of the hardest things to do is to convince small and midsize companies that they are targets—that these people even know they exist. And so, some North Korean cyber actor, a Russian cyber actor that wants to hold you ransom, that's certainly a threat. And that's one thing. But there are some that are systemically important because somewhere along the supply chain or somewhere along the influence chain or somewhere along any of these chains, even though there are small- or midsized-companies, they're important, or they could create regional havoc.

What do you think are the things we can be doing in the way we stand up this function to better convince small and midsized businesses and entities that they could become a target? They're not anonymous. Just because they're not Boeing or whatever doesn't mean they're not systemically important at the right time for the right reason.

Mr. SHELDON. Thank you, Vice Chairman.

This is, indeed, one of the biggest problems from my point of view. There are still some organizations that need to be persuaded that they are a target. But we've seen so much progress over the past few years as collectively as an industry. Academia, folks in government, including Mr. Evanina and his colleagues, have gone out and done road shows, talked with folks in industry to try and flag this problem for them.

The other piece of the problem is maybe someone's persuaded that they will be a target, and it's just a matter of resourcing the right types of tech tools, technologies, processes, and getting the right talent of people to be able to face the threat. From that standpoint, there's been some really significant progress over the past number of years about managed services that, I think, are really helping to solve this problem for people that are exploring that pathway.

If you're a small company, a dozen people or 20 people or even less than 100 people, it's very difficult to have that 24/7/365 security team that can handle an intrusion. So, a lot of people are saying, "Let's partner with an outside provider who can provide some of those things." And that helps—particularly small organizations.

So, those are some capabilities that we think are driving improvement in the area.

Chairman WARNER. Senator Feinstein.

Senator FEINSTEIN. Now, just very quickly, how do you see that the foreign intelligence landscape threat has changed since Congress last substantially updated U.S. laws in 2002? And what gaps have these changes exposed in the way that the IC views the CI mission? Whoever would like to take it?

Ms. VAN CLEAVE. Senator, I'd be happy to leap into that one.

In 2002, when the act was first passed, you'll recall that the country was in the middle of a horrible war. And this new office was stood up for the purpose of trying to deal with foreign intelligence threats at a time when most of the national security leadership of the country was seized, and rightly so, with the problem of countering terrorist organizations.

Subsequent to that time, we've seen some changes in the national security focus. But what, in fact, happened back then is that counterintelligence resources that had previously been available to deal with these foreign intelligence services were slewed over to work the counterterrorism problem. And that is in the face of having a big drawdown what we thought was the end of the Cold War of those resources—then again moved. So, if you were to look today at what——

Senator FEINSTEIN. How do you see that changing?

Ms. VAN CLEAVE. So, what I see is that we've had a change here in CI and the devotion of our resources to the mission. But, at the same time, the foreign intelligence threat has continued to be very

aggressive, very persistent, and very fruitful from their perspective. And certainly, most recently, the expansion into malign influence operations is something that is really, I think, of very serious concern to our country and to society and to our government and everyone.

Senator FEINSTEIN. And just do you see this as progress or not or the opposite?

Ms. VAN CLEAVE. Progress by the bad guys or by us?

Senator FEINSTEIN. Yes.

Ms. VAN CLEAVE. So, I think the bad guys, in fact, are making progress because we're stretched so very thin to try to deal with the threats that they present to us. And I think that our open society as a—you know, we're a bit of a candy store for them. And they're here in force. And I do think that they will continue to use those intelligence capabilities in order to advance their interests.

I'm speaking specifically now about Russia, and whatever it means for its future, and, certainly, China, and there are, obviously, others. But it's a very serious concern, and we need to take it seriously and respond appropriately.

Senator FEINSTEIN. Well, let me ask this question. Should the statutory definition of CI be updated?

Ms. VAN CLEAVE. I think the statutory definition of CI is sufficiently understood and broad to be where we need it to be. Where I would love to see some new legislative language is on the very question of what is strategic counterintelligence and——

Senator FEINSTEIN. Anybody else on that question?

Mr. EVANINA. Senator, to answer both your questions, I think the fundamental basis for this Committee's hearing today, I think when we look at the Counterintelligence Enhancement Act of 2002, a couple of things were there. It was predicated solely upon spies, you know, the Hanssen and Ames reaction, the Russians penetrating our government entities. And I think that was the premise for the act and the counterintelligence mission. That has completely changed now.

The landscape is completely asymmetric. We are less concerned about those government-to-government spies. And the battle space is now in the private sector, and it is mostly China. So, we have changed, not only the actors but the way they act here in the Nation.

Secondarily, 2002, we were just in the early stages of the Internet. So, with the advent of the Internet and the ability to scale cyber capabilities at-will of our adversaries puts, I think, the counterintelligence threat in a new lexicon that has to include cyber.

Senator FEINSTEIN. Anybody else on that question quickly?

[No response.]

No?

Thanks, Mr. Chairman.

Chairman WARNER. Senator Collins.

Senator COLLINS. Thank you. Dr. Gamache, in your testimony, you talked about efforts that Texas A&M has taken to try to secure its academic research. In your written testimony, you listed conflict of commitment, financial conflict of interest, external employment, and international travel policies as having important research security implications.

And I certainly agree with you. Unfortunately, not every academic institution is as advanced as Texas A&M in having well-thought-out policies and reporting requirements governing those potential vulnerabilities.

Do you think that the federal government, as a condition for federal funding for research, should require an institution to adopt policies similar to those that Texas A&M has?

Dr. GAMACHE. As I stated in my opening remarks, I think NSPM–33 is a start in that direction. I think academia is moving in that direction on its own from what I see. But I think there should be some guidance on what is important to protect and how we do that from a federal level.

Senator COLLINS. My experience is that academia tends to move very slowly. And we've seen that with the Confucius Institutes, for example, and how long it took colleges and universities to break their connections. Mr. Sheldon, do you have any comments in this area as well?

Mr. SHELDON. Thank you, Senator. In my spare time, I'm a professor at a university here and in DC, American University. And I know that this is just based on that experience. I know this is something that universities take very seriously. I mentioned previously that, with respect to the cyberthreat, it may not be enough to just enumerate best practices if those best practices at this point are widely known.

I think I would defer to Dr. Gamache about whether all universities that are in receipt of federal funds have a clear understanding of those best practices, or whether there's some scope for a committee or another effort of some kind to outline what those would be before making more fulsome requirements of potential recipients.

Senator COLLINS. Let me be clear that I think many colleges and universities do understand the threat, are concerned, and are starting to adopt policies that are similar to Texas A&M. But—and the Chairman has done yeoman's work with our Ranking Member, our Vice Chair, in trying to educate academia about the threat and the private sector about the threat.

But my experience is that it's been sort of this push and pull, this tugging to try to get the seriousness of the threat recognized and precautions put in place. Mr. Chairman, I do need to go vote, and I know you do also. So, I'm going to forego a second question and just ask if either of our other two witnesses has any advice to the Committee in this area.

Ms. Van Cleave, why don't you go first?

Ms. VAN CLEAVE. I don't really have anything more to add to what was just been said.

Thank you.

Senator COLLINS. Thank you.

Mr. EVANINA. Senator Collins, I'd like to add in Dr. Gamache's perspective on NSPM–33. I think it is a good start, and I do think this Committee and Congress, from a legislative body, should consider regulatory action to at least have a bare-bone minimum, especially starting with federal-funded facilities that are using U.S. taxpayer dollars to perform research that is oftentimes targeted by adversaries.

Senator COLLINS. I'm thinking, for example, of our national labs, which are likely to have far better security than many institutions. But thank you.

Chairman WARNER. Thank you, Senator Collins. Senator Wyden.

Senator WYDEN. Have you voted already, Senator Bennet?

Senator BENNET. I have.

Chairman WARNER. Would you mind yielding to Senator Bennet?

Senator WYDEN. Then if I could follow him, that'll be great.

Chairman WARNER. Yes. And then you'll follow.

Senator BENNET. Thank you very much, Senator Wyden. I deeply appreciate it.

Thank you for being here today. I think it is so important, Mr. Chairman, to have these hearings in public is so the American people can understand what some of you have described as the lack of symmetry that exists between the United States, an open democracy, and our adversaries, who are surveillance states, as the Chairman said, through no fault of the people that live in these countries. But it would be hard to describe two societies as different as the United States and China is today and what it means to our counterintelligence mission and their counterintelligence mission. To our intelligence mission and to their intelligence mission. There's almost no degree of symmetry.

If you want to comment on that, I'd be curious about what you think. We have had a generation of American politicians before us who had said, "Just wait. You'll see what happens when the Internet gets to China. They're going to democratize. They're going to democratize." Like we were saying the same thing about trade as well. And it turns out that almost nothing that we said in those think tanks or from these podiums turned out to be real. It was the opposite. China has, Beijing has, been able to export its surveillance state as a result of Internet technology and technology generally. And I wonder, given that backdrop or that set of observations, whether you could talk a little bit—I'm coming at Senator Collins's question a slightly different way—whether you could talk about what it would look like over the next decade if we actually were getting our act together here—if we were treating this as seriously as we need to treat it, if the private sector were doing—whether they were compelled to do it or not—if they were doing the right thing that our universities, our government agencies—.

What would that universe look like?

Mr. Sheldon, maybe I'll start with you, if you don't mind. If there are others that would like to comment, that would be great, too.

Mr. SHELDON. Thank you, Senator. I think that serious mobilization to the scope of the threat that you've described entails, for the part of the private sector, full and comprehensive understanding of what's at stake. And I think that from a response standpoint, that means having really robust internal security programs so that there's someone at every company, whether it's small or large, really meaningfully looking at risk. It could be risk of insiders. It should definitely be risk of cyberthreats. And then broader threats like what sort of partnerships are companies engaged in, where are they locating manufacturing facilities, where are they, who are they partnering with, and so on. And it involves integrating continual guidance from government organizations that are using their

sources and means to be able to inform how that threat will change over time.

The threats do change, because from time to time, organizations in the government will actually flag, "This is a new research priority for us, or this is a new development priority for us." And then later on, that will materialize as new intelligence tasking orders for state intelligence services.

So, it's important to have inputs from government organizations that are looking at that. It's important to have inputs from private sector and research organizations that are looking at it from their own vantage. Cybersecurity companies, for example, are on the front lines in terms of understanding different campaigns targeting specific sensitive technologies.

We do our best to work with organizations like JCDC at CISA to be able to share information about that. And there's a lot more work that we all can do as a community to make sure that, when we identify threats, we can share those. And then, companies are positioned because of having a robust internal security program to be able to action those.

Thank you.

Senator BENNET. I've got a minute left. If somebody wants to take it, or I'll give it back. Yes.

Mr. EVANINA. Senator Bennet, I think you bring up an interesting dilemma culturally for our Nation. I think when you look at—three things I could describe with your question. Culturally, we don't have an adversarial view of the Communist Party of China, which—just like we have in Russia and Iran. We have a history. You know, Cold War and the Ayatollah and the hostage-taking in 1979. We have that view. We don't have that from the Communist Party of China.

Secondarily, we grew up in this great country where we have a clear bifurcation between the government, the private sector, and the criminal element. That's not the case in the Communist Party of China. They're all together. Same thing with Iran and Russia. So, from a paradigm perspective, we don't learn that in school. And when we find out about that, it's too late. We're usually a victim of a U.S. company or institution. So, culturally, we have a lot to do, understanding those countries and how they operate different from us as a democracy.

Senator BENNET. Thank you, Mr. Chairman. And I thank the senator from Oregon for your courtesy.

Chairman WARNER. We'll go to the senator from Oregon.

Vice Chairman RUBIO [presiding].

Senator WYDEN. Great. Thank you, Mr. Chairman.

Good to see all of you. And I'm going to start with the export of Americans' private data to our adversaries, because my view is this poses a serious counterintelligence risk. This data alone or in combination with data stolen through major cybersecurity breaches threatens national security and, certainly, the privacy of millions of Americans. Now, there is, currently before the Senate, bipartisan legislation to ensure that Americans' most private data cannot be sold off in bulk to countries that would use it against us.

So, my first question, and I'd really like a yes or no answer, Mr. Evanina and Ms. Van Cleave, should our adversaries be able to le-

gally purchase bulk data about Americans, their web browsing activities, their location data, and other sensitive data?

Mr. Evanina.

Mr. EVANINA. No.

Senator WYDEN. Ms. Van Cleave.

Ms. VAN CLEAVE. No.

Senator WYDEN. Very good. Now, my second question deals with cyberthreats. The Chinese government or cyber actors based in China have hacked into Equifax and Marriott, Anthem, and OPM. My view is part of our response could be using the Federal Trade Commission, which is in a position to hold companies accountable for weak cybersecurity and also send a very strong signal to other companies that baseline security, along the lines of what, as the agency is saying, needs to be adopted. But as far as I can tell, the government doesn't really look to the Federal Trade Commission and the authorities that it has to beef up cybersecurity.

Mr. Evanina, when you headed the NCSC, did you and your staff regularly talk to the Federal Trade Commission, warn them about specific industries and firms that were vulnerable to, for example, hacking?

Mr. EVANINA. Yes, Senator Wyden, we did, as well as other regulatory agencies in this space.

Senator WYDEN. Good. Ms. Van Cleave, same question.

Ms. VAN CLEAVE. Senator, when I was in that job, we didn't have a security portfolio. We were responsible only for—quote/unquote, only—for counterintelligence, which meant that, no, we didn't have interaction with organizations like the FTC.

Senator WYDEN. Do you wish you had that authority?

Ms. VAN CLEAVE. Well, I don't know. I think that the responsibilities for security and for enhancing our security across legal and other measures are broader than one organization alone. And I have to say, contrary to people who look at a job and want to build the empire larger, I thought I had my hands full as it was, taking on the CI mission, and I'd look to others to handle the security responsibilities.

Senator WYDEN. No, I get your point. It's just that if you have a sister agency that can hold companies accountable, which is one of the charges of the FTC, I'd like to see us use it.

One last question, if I might, for you, Mr. Sheldon. You've expressed concern about requirements to provide nonpublic encryption information to governments and about the governmental imposition of "excessive lawful access requirements." And you characterized this, I gather, as "a form of mandated vulnerability by coercion." And you focused, of course, on the People's Republic of China.

Now, is it correct to say that requirements by any government, including our own, to impose vulnerabilities in encryption are a threat in our ability to defend ourselves from sophisticated adversaries who are looking to exploit those vulnerabilities?

Mr. SHELDON. Thank you, Senator Wyden. The statement in my written testimony that you're referring to was directed at foreign adversaries. I've spent less time looking at this issue on the U.S. side.

Senator WYDEN. Okay. Again, I would say the requirements by any government to impose vulnerabilities in encryption, I think, make our country less strong. You know, there has been all this debate about encryption and: is it for security or is it for liberty? You know, the fact is we are safer with strong encryption. And it is, I think, a tool that has to be an imperative for America's security in the future.

Thank you, all, for being with us.

Mr. Evanina, I'm just going to close with one last point, because I asked the staff about it. We were looking for your responses to the questions for the record that we sent after a previous appearance. If there's any way that you can do it, this is not to give you a hard time or anything, I'd like to see those answers because I respect your opinion.

Vice Chairman RUBIO. Thank you. Senator Blunt.

Senator BLUNT. Thank you, Senator Rubio.

Let's talk a little about campus security and research security on campuses largely, I think. Dr. Gamache, you have the professional designation on security, and you're representative of an academic institution here. What are the best and worst practices you've seen from the federal government trying to be helpful, or, on the best practices side, I guess it would be being helpful? Give me some of the things you've seen that you thought were the least effective and most effective.

Dr. GAMACHE. In terms of awareness, I think some of the things that are least effective happen when government agencies try to do a search-and-replace with industry for academia. You know, I think a lot of the things that we see from the government in academia don't reflect a real understanding of the academic culture.

We have the greatest higher education system in the world for a number of reasons. We've got an open and collaborative environment. We have a willingness to collaborate internationally. We have a desire to push science and the creation of knowledge as—as far as we can.

We have cutting-edge technology. That is all very, very important to our standing as the best in the world. And I don't think what we see coming from the federal government all the time reflects an understanding of what makes us strong. I would hate to see a mandate break the system, for lack of a better word, trying to fix it.

Senator BLUNT. What about the best thing you've seen, the most helpful thing?

Dr. GAMACHE. You know, what I have seen over the last five years is kind of a mind shift from a number of agencies who have really tried and worked hard to understand what the academic community is all about. And, I'll single the FBI out, in particular. I think they have worked very hard with us to understand academia.

Recently, the Department of Commerce has reached out to do the same thing. Academia created a group back in 2017 called the Academic Security and Counter Exploitation Program. We have about 200 universities involved in that right now. We have 10 major universities on our executive committee, and we've got six government agencies that are involved in that as well.

So, I think that collaborative effort between academia and the federal government down at the grassroots level is really paying dividends in terms of awareness.

Senator BLUNT. So, both of those sort of reflect the same thing. And it's understanding culture——

Dr. GAMACHE. Right.

Senator BLUNT [continuing]. Before you decide how you're really going to effectively deal with the institution.

Dr. GAMACHE. Yes, sir.

Senator BLUNT. Mr. Evanina and Mr. Sheldon, what are your thoughts about how we get people there in the nongovernment sector who are targets to recognize the fact that they are targets? What are some of the things you'd suggest we do a better job of helping targets know they could be targets or maybe that they already are targets and haven't determined that yet?

Mr. Sheldon.

Mr. SHELDON. Thank you, Senator.

I think that a lot of people who are being heavily targeted right now know that they're being heavily targeted, and they're investing in security programs to try and stop it. I think there's still work to be done to make sure that everyone who's being targeted has a clear sense of that.

And I think that to the extent that, we, either in industry or folks in government, can provide real, actionable advisories about when adversaries shift that targeting or where a new priority emerges that is attention-getting. And I think that there are examples of times where we in industry have published white papers or blog posts that said some specific type of technology—might be additive manufacturing, might be satellite communications, might be any number of other specific things—being targeted by a specific campaign or threat actors maybe from China, maybe from Russia. That tends to get attention and drive action.

But it has to be very specific. There is a little bit of alert fatigue at this juncture here where we stand in 2022, where people have been told that they need to be concerned about cyber for a long period of time. So, if we don't get really targeted messages to people that apply to them, they may find themselves ignoring it. But if you name a specific technology that a small company is working on, researching, and they just invested a lot of effort and a lot of resources in bringing that to market, and you're able to point to that, that tends to catalyze action.

So, government and industry can both make progress there.

Senator BLUNT. Thank you.

Mr. Evanina, do you anything to add to that?

Mr. EVANINA. Just to amplify: outreach at scale. I think a true public-private partnership between the government and a private sector consortium to advise and inform companies, large and small, to the small-time manufacturer in Kansas to Microsoft and Google, what those threats are. That's scalable as well. Where do you find that direct information that's not only real-time but actionable for small companies and medium-sized companies? And as we've seen in the last few years, every company is vulnerable and every company will be penetrated.

Senator BLUNT. But Mr. Sheldon's concept that if you know there's something out there that our adversaries are really interested in, to let people who are working in that area know that. Is that something we're doing effectively?

Mr. EVANINA. Yes, Senator Blunt. I think, as I wrote also in my statement for the record, the government, the "big government," must be more effective and efficient at notifying industry of those threats when we see them in a classified manner. The more effective way to declassify in real time, to be able to provide that industry of a specific company—similar to what we do in terrorism—needs to transition here, and the nation-state threat actors as well.

Senator BLUNT. Thank you. Thank you, Chairman.

Vice Chairman RUBIO. Senator Casey.

Senator CASEY. Thanks very much. I want to thank the panel for your testimony your presence here today.

Mr. Evanina, I have to point out your roots in northeastern Pennsylvania, Peckville, Pennsylvania. We share the same home county, Lackawanna County. So, I want to note that for the record. And thanks for your service and the work of everyone on the panel.

I wanted to start with legislation that I worked on with Senator Cornyn. The two of us have been leading this legislation in the Senate for a good while now. Senator Rubio and others have worked with us on this. And it's a piece of legislation called the National Critical Capabilities Defense Act. What we're trying to achieve with this legislation is to have an outbound review of investments so that we can focus on either services or assets that are vital to the United States national security, whether it's agriculture security, health security, homeland security, energy, infrastructure, natural resources. It goes on and on.

We haven't been successful at getting it enacted into law yet, but we're getting close, or at least a version of it. And I guess one question I have in light of the discussion is whether or not—and I'll start with you, Former Director—could NCSC, or the IC more broadly, help to educate the private sector with regard to the risks of outbound investment, especially when it comes to China or other foreign adversaries?

Do you think there's a role for either the IC more broadly or NCSC, and especially in the early stages of technology development?

Mr. EVANINA. Senator Casey, thanks for the question. And pleasure to share our home county.

The answer is yes. And I do believe there's success currently—the way it's done in the Intelligence Community on CFIUS, and the way that the Intelligence Community partners with Treasury and Commerce and others to identify potential investments in the United States. And I do think this legislation reverses that to say the same type of vulnerability and threats to national security occur outbound, especially investment in Asia, China and other entities that have vulnerabilities.

So, I do think there's a role for the government to play in that space, specifically whether it's NCSC or the ODNI. But for sure, the Intelligence Community, with real-time threat indications or warning, can certainly advise you and inform an investor of the perils of investing overseas.

Senator CASEY. Anyone else on the panel on this question in terms of a perspective on it?

[No response.]

Let me move to my second question—I think it would be my only other question—which is, in terms of all the challenges you've outlined in your testimony to society more broadly, whether it's the academic community, academia itself, or the private sector—I want to put the ball back in the court of Congress now and ask you what other incentives or resources do you think Congress can provide to help these non-IC entities to better protect their—whether it's intellectual property or research or technology or otherwise?

Maybe, Mr. Sheldon, we can start with you and go right to left.

Mr. SHELDON. Great. Thank you, Senator.

I want to flag a couple of things I think we're doing well. So, I mentioned this previously, but I think we're doing a good job, as a community, really raising awareness. So, that's helpful. And I think there's been some new structures that have come up in government now to help with collaboration and coordination, in particular, on cyberthreats. So, I think that we're making progress there.

Further, I could say, I think there's also some new requirements either from the SEC or on incident reporting through CISA that are going to really force companies to be more forthcoming if there's been issues that might be important for national security and disclose information about those. That should help organizations like the SEC and CISA provide good information and advisories to the community. I think it's now likely time to start the conversation about what extra resources can we bring to bear to actually provide cybersecurity capabilities to companies that need it and can't get it for whatever reason.

Normally, it's because of resource constraints. So, I've mentioned a couple of things in my written testimony that, I think, are worth like [inaudible] are worth exploring. One of those is trying to look at tax mechanisms to try and understand if there's a way that we can get small businesses, in particular, technologies like managed security services so that they can actually meet the threats that they face.

And another one would be just having a program that could create more incident response capacity. So, if there is an issue of some kind that we, as a Nation, have enough resources standing by to be able to meet those threats?

Thank you.

Dr. GAMACHE. I would like to echo the theme of resources. You know, we have a staff within the A&M System of 19 that are looking solely at the research security effort and the cyber piece that goes with that. It's all being taken out of hide because we believe it's important. But as we get more and more requirements like NIST–800–171 and what's coming down now within NSPM–33. We're a well-resourced university system. Smaller colleges have the same requirement to protect that information but can't make the same business case that we can. And I think that needs to be taken into consideration.

Ms. VAN CLEAVE. Senator, I think that there are a lot of new creative solutions with respect to security where there is a lot of work

being done in the private sector and in government that that needs to continue. For example, within the Defense Department, there is a program called Deliver Uncompromised, which looks to all of the providers, the contractors, for the DOD to come look at security as an objective to be achieved rather than a cost to be minimized.

And so, when you start having practices like that, I think you're going to improve things overall. But I would note that one can continue down the road of security—as we must, to improve it—as we must, to come up with better ideas—as we must. And yet, there will always be a determined adversary looking for ways to break through.

So, if you ask what is it that Congress can help do, Congress can help refocus on the core counterintelligence mission that says the role of the U.S. government—in addition to advising business, industry, and academia and all the things it needs to do to protect itself against—the role of government uniquely, that we can't ask Texas A&M to do and we can't ask CrowdStrike to do, is to go after the bad guys.

And we are failing in that mission right now, in my opinion, sir.

Senator CASEY. Thank you.

Chairman WARNER [presiding]. Let me pick up on this. I got a couple more questions, notion of responsibilities. I appreciate Dr. Gamache, and we are saying that correctly, right? I want to make sure that we're right. We have not all completely butchered your name for two hours here.

Dr. GAMACHE. Yes, you are.

Chairman WARNER. Thank you.

You know, on this cascading issue from large systems like Texas A&M to a smaller liberal arts college, you know, we see it in the cyberspace as well, from incident reporting or—one of the areas that this Committee again wrestled with. And we all said, you know, you got to have at least de minimis cyber standards within all the centers on the Internet of Things. And trying to get people to adopt that has been, I think, a real challenge.

You know, one of the areas—you know, Senator Wyden is always keeping us on our toes on kind of privacy issues—but one of the things that I don't think we do a very good job of at all, and it's almost like—not that the IC is reluctant to look and the FBI is reluctant to look—is just looking back at the supply chain. If you look even from our defense contractors where not first tier or second tier but third tier in smaller suppliers where some of that originates. I think, again, COVID exposed so many vulnerabilities from Russia and China. There are some private sector companies out there doing that now, but do we need to rethink authorities on this issue to allow the IC—. In a sense, how do we grapple with it? Looking at a question like supply chain, having the IC look at an otherwise well-functioning company, no sense of them being targeted, although we know almost all these companies are, and go back in terms of their sourcing of their materials. That would make a lot of folks in the IC right now very uncomfortable.

Do you think that's something that we ought to have a requirement? And where would you put that?

Ms. VAN CLEAVE. Mr. Chairman, if I might offer a perspective on that. When I was serving in the counterintelligence office, we were

assigned the responsibility of providing intelligence support to CFIUS, as CFIUS was making the decisions about what constituted a national security concern. And I will tell you that the problem is, when you go to the Intelligence Community and you say, "Please show me what you got on Company X, Y, or Z," those files are not going to be very comprehensive. And that's because we haven't really looked at these targets for intelligence assessment purposes in order to be able to understand those operations. And so, there is a tug and pull on how you want to array your intelligence resources and what the priorities are. And perhaps there's an opportunity to prioritize these things a little more than we have——

Chairman WARNER. Although there's the challenge that because we don't generally want the IC looking at domestic, obviously, domestic persons but also some domestic content, the ability to kind of go—CFIUS or otherwise—up the food chain, I think some of the large enterprises, even in the defense area, don't know where their third-tier suppliers are originating.

I think some of these private sector companies are exposing that, or the ability, particularly of the CCP—I think we became alerted to CCP direct investments in America. And I still remember one of our roadshows in Texas, actually, Dr. Gamache, where some small AI company said, "Well, I wondered why the Chinese VC was paying three times more than anyone else." And we didn't have that information. And the CCP has gotten smarter where they now may invest, not through a Chinese-based entity, but through some European subsidiary and entity, and our ability of trace, again, up the food chain is really challenging.

Bill, did you want to comment on that?

Mr. EVANINA. Senator, I do think that if we are going to get to a place where we could have an effective supply chain risk mitigation program, or even get to zero trust, we have to have a carveout somewhere where the parts of the Intelligence Community can play in the space and be comfortable advising and informing U.S. industries that there is a threat, or there is a vulnerability in a coding aspect, or somewhere along the IT supply chain or in the procurement supply chain. That's very easy to do, just a matter, to your point of the uncomfortable nature of the IC getting involved in that is natural and it's prudent. I just truly think that if we're going to move in a place where we can have a protection of our supply chain, the IC is going to have to play because they have left-of-boom activity and intelligence collection they could share with those entities.

Chairman WARNER. I think, again, there's both that ability to look at—from a national security standpoint. Some of that, up the domestic supply chain in terms of origination, I think, is important. I also think it's something we've stressed a couple of times here. I think we did. And with your help, do a good job of those classified roadshows.

In many ways, they needed to be classified, though, because at just the non-classified level, if you can't share the experiences, the enterprise or industry sector may not—they might say "What do you mean?" We can't give them some details. But I wonder, at

times, if we had not initiated that, if we'd left it to the—I think the FBI stepped up their ability to make those presentations.

But again, I think because we took the bull by the horns or whatever the analogy is, but I'm not sure that's a systemic way to address this on informing our folks. So, that leads me to the question, which I would have some trepidation on, but one of the things around this whole CI mission, and I'm not sure where I'm going to start on this one, but do we try to look at the British model where they actually have a domestic counterintelligence entity?

Now, clearly, the U.K. has a whole set, a different set of—. We have a whole set of protections, First Amendment and otherwise, that I think make our system better. But, you know, they have Scotland Yard, and yet they have MI5.

Maybe I'll go the reverse route again this time.

Is it time to look seriously at the idea of an independent counterintelligence entity in the United States?

Mr. SHELDON. Thank you, Mr. Chairman.

I think, from my perspective, there are other folks on the panel that are better suited to address the organizational question.

I just want to add quickly that for some aspects of industry, especially industry where you have international clients and business, maybe places in Europe and elsewhere, it's more straightforward to liaise for the purposes of something like JCDC with an organization that is removed somewhat from the Intelligence Community, because that makes everyone's customers more comfortable. So, that's an important equity to protect if there's going to be a reorganization. It's just to ensure that there are ways to collaborate between industry and government through more civil authorities.

Thank you.

Chairman WARNER. And I think, again, it's still a work in process, but CISA—. You know, I think I was wrong that having CISA have enforcement proceedings against people who fail to incident report is the wrong approach because CISA ought to be that friendly entity that is not in the regulatory sense, but—.

Dr. Gamache.

Dr. GAMACHE. I would defer on the organizational portion of that, Senator, but I believe that there has to be a way to plug academia into whatever solution you come up with.

Chairman WARNER. Michelle.

Ms. VAN CLEAVE. Mr. Chairman, I do have some strong views on this, actually. In my view, one of the strengths of U.S. counterintelligence is the diversity of talents and skills and approaches and training represented in the very different agencies and the responsibilities that they have had across our government. There's value in having a national counterintelligence service, as most other foreign governments do have a centralized service.

But I think that we have untapped potential in the fact that we've got such a tremendous variety of people and skills. The missing element is the ability for select high-priority targets in a strategic way to meld those things together, those activities together, so that they can operate as one team with one plan and one goal when required.

That's the missing element, in my opinion.

Chairman WARNER. Bill.

Mr. EVANINA. Senator Warner, I'm going to wrap a few things together and get back to Dr. Gamache.

First of all, I do think our higher education should be looked at as part of the national security and defense program. I do think that it's worthy of putting it in a bucket with other entities we spend money to protect, number one.

Number two is, if you just juxtapose when we talked about the changing landscape of counterintelligence over the last two decades, I would proffer to this Committee, if you look at our counterintelligence strategy now, protecting critical infrastructure, ensuring a supply chain, economic security, malign foreign influence, who has the authority legislatively to handle all those parts of the defense process?

They're Whack-A-Mole through different organizations. And I do think that if we are going to modernize the concept and lexicon of counterintelligence, we have to look at what's being affected here in the U.S. And it comes to cybersecurity. At the end of every single breach that Mr. Sheldon talked about, there's a human being somewhere and a keyboard, either in China or Russia or Iran. So that cannot be forgotten.

I think when we look at how we structure this, we have to look at—the 2002 Counterintelligence Enhancement Act did not take all these things into play. It was more spy versus spy. So, I'm not sure an MI5, MI6 model is required. I do think we have existing structures that are probably predicated in a 1980s mindset, but I do think we have to find the way to fill in the gray space to protect where the battlespace is now in the private sector.

Chairman WARNER. You know, one of things we want to try to do is solicit input, but I start with a, for a variety of reasons, prejudice against a new entity. And I am very conscious—, you know, we think about some of the prominent American companies when we got into AI, and sometimes, they were reluctant to work with the community. I think many of the Members of this Committee believe that this is such a technology competition now, beyond the traditional mill-to-mill and identifying that technology where we're going to go deep. I think we have done a little bit on the 5G piece and the chips piece.

The Committee, in a bipartisan a way, has agreed to look at synthetic and bioprocessing series areas there and things around advanced energy to think about those because they would not have been in the category of a traditional national security, counterespionage, intel agenda ten years ago, maybe not even five years ago, but I think clearly are now.

Ms. VAN CLEAVE. Mr. Chairman, if I might just?

Chairman WARNER. Yes, please.

Ms. VAN CLEAVE. To interject, and before this comes to a close, and thanking you again for your leadership and for your decision to hold this hearing and the subsequent hearings that you are planning on counterintelligence. There is one point that I believe I would be remiss if I didn't speak to the record on this point.

And that is that I want to assure you and the Committee that, sadly, traditional espionage is still ongoing. It is still directed against us. It is still very much a threat to our national security,

to the secrets that are most important to our national security, to the people and treasure who work with our Intelligence Community, to our troops in the field. These kinds of penetrations into the U.S. government that are traditional espionage is very much ongoing. It is very much the focus of our adversary, and I would urge, as the Committee moves forward, to keep your eye on that as well.

Chairman WARNER. Oh, we are very aware, and this kind of open setting is not the place to go into that. But even in terms of some of our near-peer competitors, just the number of people they have in-country under some level of traditional diplomatic status, whether their embassy or through the UN, is a huge issue.

It is not an either-or proposition. I know there are a number of other Members—with the vote schedule, sometimes, it is a hodgepodge—but I very much appreciate everybody's presentation, and obviously, we've got some more work to do. Committee is adjourned. Thank you all.

[Whereupon the hearing was adjourned at 4:21 p.m.]

Supplemental Material

MICHELLE VAN CLEAVE
Answers submitted in response to questions for the record

U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE
September 21, 2022
Open Hearing on Protecting American Innovation:
Industry, Academia, and the
National Counterintelligence and Security Center

Changes in the Counterintelligence Mission

1. **Should the statutory definition of counterintelligence be updated to include foreign malign influence and malicious cyber activities?**

In my view, the current statutory definition of counterintelligence (CI) [1] is broad enough to encompass malign influence and malicious cyber activities to the extent that CI has a role to play in countering them. Unlike *espionage* directed against the United States, these threats are not the exclusive concern of counterintelligence, but by law fall under multiple authorities. For example,

- Under current law, the Foreign Malign Influence Response Center (50 USC 3058) is to be composed of personnel from all elements of the intelligence community (IC), including those with diplomatic and law enforcement functions.
- Lead authorities over counter-cyber operations are vested in the Secretary of Defense (10 USC 394), who shall "conduct military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power." Those authorities explicitly include "operations in cyberspace short of hostilities."

While it might be helpful to clarify that the term "other intelligence activities" in the definition of counterintelligence includes malign influence and cyber activities, the new statutory language (or accompanying report) should reflect that countering these foreign threats is not exclusively a CI mission.

2. **How should strategic counterintelligence be defined in statute?**

The principal responsibility of counterintelligence, whether strategic or tactical, is to engage and confront the adversary, which means carefully orchestrated, proactive operations to influence, compromise, or disrupt hostile intelligence threats.

---

[1] 50 USC 3003(3): *The term "counterintelligence" means information gathered, and activities conducted, to protect against espionage,* **other intelligence activities,** *sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.* [Emphasis added]

As I understand the term,[2] what makes a CI effort "strategic" is the means-to-ends analysis (strategic operational planning) that identifies and assesses the "red" (Foreign Intelligence Service) "order of battle" (adversary plans, intentions and capabilities) and arrays "blue" (U.S. CI) assets to achieve defined objectives. In testimony, I offered the following draft definition:

> 50 U.S. Code § 3003(4) – Definitions. As used in this chapter … *(4) The term "strategic counterintelligence" means the direction and integration of counterintelligence activities to disrupt or compromise the ability of foreign intelligence services to harm U.S. national security interests at home or globally.*

If the United States is to have a national strategic CI capability, we will need some fundamental new elements, including a purposefully designed strategic CI program. But first, our national security leadership, and the professionals who lead U.S. counterintelligence, need an agreed understanding that such a national effort is in fact the goal. Defining the term in law – as the Committee's organizational assessment of the National Counterintelligence and Security Center (NCSC) recommends[3] -- would be a very constructive first step.

The U.S. CI Enterprise

3. Which legal responsibilities should non-IC entities—including U.S. government agencies, academic institutions, and private sector companies—have to protect their intellectual property, research, technologies, and data with national security implications?

Government as well as private entities should and do have full legal and practical responsibility to develop and implement security measures to protect their sensitive data, facilities, operations, etc., whether the threat actors are domestic or foreign. They are in the best position to know what is of value and therefore what needs protection, to determine their level of risk (because they know the value of their strategic information, and they know their business), and to apply the security and countermeasures required.

While sound protective measures are unquestionably vital, they are only part of a broader effort to protect our nation's R&D base and other critical information against illicit foreign exploitation. We also need good counterintelligence, meaning that the U.S. government needs to be much more pro-active in identifying, assessing and disrupting foreign intelligence operations against us. Without the tools the U.S. counterintelligence enterprise alone can and must provide, we will continue to lose ground.

4. Which incentives and resources could Congress provide to help non-Intelligence Community entities better protect their intellectual property, research, technologies, and data from foreign adversaries?

---

[2] See for example Michelle Van Cleave, "The Question of Strategic Counterintelligence: What is it, and what should we do about it?" *Studies in Intelligence* 51, 2 (Washington DC: Center for the Study of Intelligence, Spring 2007) 1-13

[3] Senate Select Committee on Intelligence, *Organizational Assessment: The National Counterintelligence and Security Center,* Audits and Projects Report 22-01, United States Senate (2022), p132

The single most important resource Congress could provide is to establish in law a strategic CI program, managed by the head of U.S. counterintelligence and empowered to identify, assess and disrupt foreign intelligence operations directed against our commercial wealth, R&D base, critical infrastructures, democratic institutions, and sensitive national security information and activities. In testimony, I offered this draft mission statement:

> U.S. Strategic Counterintelligence shall degrade the ability of foreign powers to project force or prosecute national objectives; establish or maintain hostile control; or securely conduct operations or collect intelligence and other information against U.S. interests globally, by means of their intelligence activities.

5. What are the biggest challenges academic and private sector entities face in confronting foreign adversarial intelligence collection and economic espionage?

In order to protect themselves, America's universities and private enterprises need to be aware of the activities of foreign entities directed against them. For example, what are the practices and techniques of foreign intelligence services and their agents in acquiring proprietary and other information? Are they exploiting front companies, if so, which ones and how? What are their recruitment techniques? Their solicitation operations? Who and what are they targeting?

This is the kind of threat information that the FBI endeavors to provide to academia, business and industry, so their security professionals can do the realistic risk assessments required to protect the things they value. In my view, however, we have not invested nearly enough effort (funding, manpower, program execution) in identifying and assessing foreign intelligence operations, much less the CI operations needed to defeat them. Unless U.S. counterintelligence is able to gain better actionable insights into adversary intelligence activities, we will continue to lose ground.

6. Given the generally lawful nature of foreign acquisition of U.S. technology, does Congress need to consider additional updates to the Committee on Foreign Investment in the United States (CFIUS) to address remaining loopholes?

The welcome passage of FIRRMA in 2018, coupled with President Biden's new Executive Order 14093 (September, 2022), have given greater reach and specificity to CFIUS reviews and filing requirements, along with a schedule of penalties for failing to honor mitigation agreements. Whether those measures will be adequate remains to be seen, and at a minimum warrants Congressional monitoring with an eye toward additional updates as required.

The core challenge for CFIUS remains defining what constitutes a national security concern, on a case-by-case basis, and weighing that against our fundamental belief in free trade and open commerce, for the purpose of advising the President what to do. One major test case may well be the consortium (led by Elon Musk) that purchased Twitter earlier this year, which reportedly includes a number of foreign investors.

One of my responsibilities as the National Counterintelligence Executive (NCIX) was to provide analytic support to CFIUS concerning the bona fides of foreign investors seeking to acquire an interest in sensitive industries in the United States. At the time, I was concerned that in too many

cases the intelligence community lacked the insights necessary to make key judgments about these critical business dealings with sufficient confidence to enable informed decisions.

In order to exercise his authority under CFIUS, the President must have "credible evidence" that the foreign interest exercising control may take action detrimental to national security. That in turn requires that U.S. intelligence and counterintelligence be tasked and resourced to collect on those foreign interests. As the Congress considers updates to CFIUS, the Oversight Committees may also want to review whether those collection and analytic resources are adequate, not only to support CFIUS deliberations but for other actionable purposes as well.

7. How can the U.S. government best strike a balance between protecting national security and preserving a culture of international collaboration, free enterprise, and open research?

Having had the privilege over the years of working with some of our Nation's extraordinary scientists and engineers, I know the ethic and culture of openness that surrounds research and development are essential to nurturing ideas, innovation and progress. I am very respectful of these values, and I share them in full measure.

Unfortunately, the rich network of human interaction that is innocent and open and above board provides excellent cover for the sliver of activity that is none of that. Foreign collectors trained in the art of elicitation know how to obscure their true interests in a cushion of seemingly innocuous exchanges. They routinely exploit joint research undertakings or visits to U.S. businesses, defense contractors, military bases, research facilities, or academia, in order to obtain non-public information that may be valuable in itself, or provide leads to more sensitive sources or insights. The use of cyber tools as a collection modality is of particular concern, especially where informed or facilitated by human sources.

I don't know where the balance should be drawn, but I believe that it should be possible to find a balance that respects and supports our basic values. Within the United States we believe in the free flow of information, but we don't believe in insider trading. We believe in patents and copyrights that protect intellectual property. We believe in respecting the confidentiality of privileged communications. In short, we do recognize important constraints on the free flow of information; the increasingly urgent imperative is to extend like reason and fairness to the protection of our nation's critical information.

8. What can be done to enhance U.S. government agencies' ability to conduct investigations into grant fraud and technology transfer, in collaboration with universities?

I do not have any current insights into these criminal investigations, but would respectfully refer the Committee to the relevant law enforcement agencies (FBI, DOC/BIS, DHS/ICE, DoD/DCIS and the military service components) for their views.

9. Should non-Intelligence Community agencies establish their own counterintelligence and/or security programs? If yes, what should those programs look like? If no, should the FBI or other Intelligence Community entities perform that role?

Counterintelligence is inherently an intelligence mission ("*information gathered and activities conducted*" to counter foreign "*intelligence activities*"), which by definition is not the responsibility of non-IC agencies. By contrast, security is a distributed "command" or line function, for which each government agency (whether or not part of the IC) is separately accountable.

While there is always room for improvement, rigorous requirements for protective security programs are already in place and binding on non-IC agencies. For example, all government agencies with access to classified information are required to meet standards for detecting and mitigating insider threats (E.O. 13587). Security measures to protect national defense (i.e., classified) information are established by the DNI and binding on all who have access to such information, including such things as background investigations and adjudication standards for granting clearances as well as requirements for the retention and protection of classified documents both physical and digital (ICD 700 series). And all government agencies are responsible for establishing and executing security plans and programs to screen employees (based on position sensitivity and risk) for suitability, and to protect their sensitive information and operations (see for example E.O. 14028 "Improving the Nation's Cybersecurity").

By contrast, the defining job of counterintelligence is to engage and confront the adversary. To that end, the responsibility to identify, assess, and disrupt foreign intelligence services (including their agents and proxies) targeting U.S. national defense information, economic wealth, or democratic institutions, falls to those highly specialized CI agencies manned, trained and equipped expressly for that purpose and so designated by law and executive order (principally the FBI, CIA, and the military services).

I support the recommendation in the Committee's assessment of the NCSC[4] that the distinction between counterintelligence and security be codified in law. These are mutually reinforcing missions, yet each has separate and distinct roles, authorities and objectives, requiring very different resources, capabilities and metrics. The NCSC also needs to help clarify these distinct roles and missions so that each can be assigned, tracked and performed to best effect.

10. To what extent should the State Department vet foreign students, professors, or employees from a counterintelligence perspective?

Adversary intelligence services often use academics as well as businessmen and others to facilitate their operations within the United States. First line responsibility for vetting foreign visitors to the United States is assigned to U.S. Immigration and Customs Enforcement (ICE), Department of Homeland Security, as part of the visa application process. Where the need for additional scrutiny is indicated, applications may be referred to other government agencies (e.g., FBI, CIA) for review. Within the State Department, the Bureau of Diplomatic Security, deployed at consular posts abroad, is responsible for investigating suspected passport and visa fraud. I would respectfully refer the Committee to the respective government agencies for their views on whether these reporting channels and information sharing arrangements are being used to best effect.

---

[4] *Ibid*

11. Should academic institutions do their own research security vetting of visiting students, professors, and employees?

a. What tools, resources, and support from the IC would be needed?

Yes. Any institution of higher learning has a vested interest in ensuring visiting students and faculty are not abusing their academic affiliation for unlawful purposes. Alerts published by the federal government attempt to raise awareness of the ways in which foreign intelligence entities (FIE) exploit these ties.[5]

12. How can the U.S. government in general and the Intelligence Community in particular better communicate the foreign intelligence threat to the American public, private sector companies, and academic institutions?

Each year, reports out of U.S. counterintelligence show figures that are worse than the year before. Losses are growing. Numbers of foreign collectors are growing. Vulnerabilities are growing. And the erosion of U.S. security and economic strength is also growing.

Yet neither the recently issued *National Security Strategy of the United States*, nor the 2022 *National Defense Strategy*, addresses the threats posed by hostile intelligence services. If the American public is to have a better appreciation of what is at risk, and what is being lost, and what needs to be done to protect what we value, then our national leadership needs to give these matters the policy priority and prominence they deserve.

I would invite the Committee's attention to the fact that, as of this writing, President Biden has yet to name a head of U.S. counterintelligence. If the administration is serious about engaging the private sector in confronting foreign intelligence threats, filling this key leadership position would be an obvious place to start.

13. How can the U.S. government in general and the Intelligence Community in particular partner with non-Intelligence Community entities to prevent foreign intelligence penetration and exploitation?

a. To what extent should the Intelligence Community be proactively protecting non-Intelligence Community entities through offensive counterintelligence operations to disrupt foreign adversary targeting of those entities or cyber support to prevent foreign adversary penetration and exploitation of online systems?

Preventing foreign intelligence penetration and exploitation of our nation's sensitive information and operations is job one of U.S. counterintelligence. Unfortunately, America's CI enterprise is not structured to go on the offense.

For much of its history, U.S. counterintelligence has been principally defensive and inward looking. Our default position has been to wait until the foreign intelligence threat is inside our borders before taking action, where the bulk of that responsibility has fallen on the FBI. Here,

---

[5] See for example Defense Counterintelligence and Security Agency, *Foreign Intelligence Entities' Recruitment Plans Target Cleared Academia* DCSA-AD-21-001, Department of Defense, April 2021

foreign adversaries have found America's free and open society a target rich environment, expanding their operations as the funding and effort we devote to countering them have declined.

To make matters worse, the modalities and vulnerabilities enabled by the information revolution -- and its evil twin the disinformation revolution -- have amplified the price we pay for inadequate counterintelligence, as our very democratic institutions have been put at risk. What has been missing – before and after cyberspace reshaped our world -- is an integrated, nationally-directed strategic CI program.

Executing an offensive CI strategy against adversary intelligence services would require a new way of doing business, beginning with working the target abroad. The considerable resources of the members of the U.S. intelligence community that have global reach would need to be directed to help identify and then disrupt or exploit foreign intelligence activities, wherever they are directed against U.S. interests worldwide.

Likewise, the best cyberspace defense is likely to be a good offense. From a counterintelligence perspective, the key is getting inside the attacker's intelligence operations to find out what they are doing and how they are doing it, in order to stop them, confuse them, and otherwise tip the scales in our favor.

The missing element is a national CI program to enable the integrated planning, orchestration and execution of strategic CI operations to identify and disrupt hostile intelligence threats, whether directed against U.S. national security secrets, business and industry, critical infrastructures, or our democratic institutions.

NCSC'S Mission

14. What should NCSC's mission be going forward?

In my view, the original purpose for which the national CI office was created remains as compelling today as it was 20 years ago when President Bush first appointed me to the job.

Congress created the NCIX (predecessor to the NCSC) because foreign intelligence services were exploiting the seams in U.S. counterintelligence at a painful cost in lives and treasure. The mission of the NCIX (which is still governing law) was to serve as the head of U.S. counterintelligence – a first for the enterprise. The NCIX was responsible for providing strategic direction, and integrating CI activities across the federal government (principally the FBI, CIA, and DoD/military services) through threat assessment, budget and program guidance, training and education, and operational prioritization.

However, while charging the NCIX with that mission, Congress did not create a national strategic CI program that the NCIX would be empowered to manage. In other words, it created a national Executive but not the means of execution.

As a result, we have a national CI strategy, but we do not have a strategic CI capability. The DNI's decision in 2010 to consolidate CI and security responsibilities under a single national center has resulted in the NCSC spending the bulk of its time and effort on security, rather than the very different challenges of counterintelligence. The unity of effort and priority requirements of

strategic counterintelligence have yet to find expression in ordering the plans, programs, budgets or operations of the component CI agencies.

Any strategy is useless unless it connects means to ends. For that to happen, people need to be held accountable for employing the resources they control to achieve those ends. These are the qualities of a program. And they are qualities the national counterintelligence mission does not yet possess.

Going forward, the NCSC should be revalidated and empowered to perform the mission originally assigned. Most importantly, the NCSC needs to lead the transformation of the CI enterprise to be able to work as a cohesive whole. To that end, I recommend that Congress establish in law a strategic CI program, managed by the head of U.S. counterintelligence, to marshal the resources of U.S. counterintelligence to find out what hostile intelligence services are doing, and how they are doing it, in order to stop them.

15. Should NCSC focus on coordinating and integrating traditional counterintelligence activities and operations across the Intelligence Community or establishing a strategic counterintelligence program for the U.S. government as a whole?

To a large extent, these are one in the same. Any national strategic CI program will require the coordination and integration of traditional CI activities and operations across the government to achieve a common goal. What has been lacking is an agreed understanding on that common goal.

U.S. counterintelligence is finely tuned to work individual cases, but it is not postured globally to disrupt a foreign intelligence service. CI resources have been concentrated within the United States, allowing the adversary to bring the threat into our backyard. While there is bilateral deconfliction, CI agencies work independently to meet agency-specific objectives.

Without prejudice to standing agency responsibilities, the national CI enterprise needs a new business model to provide the strategic coherence to go on the offense against select targets. Under the leadership of the NCSC, a strategic CI program, comprising dedicated elements across the CI community, would consist of three parts:

- Develop foreign intelligence service "order of battle" through focused collection of adversary plans, intentions and capabilities, identification of intelligence gaps, and assessment of adversary vulnerabilities
- Conduct strategic operational planning to redirect or reallocate U.S. collection and operations against this now understood target set based on our capabilities and opportunities for interdiction or exploitation
- Integrate and orchestrate CI resources to achieve these strategic objectives, with operations assigned to the appropriate CI entities.

16. How should NCSC coordinate and de-conflict efforts with the FBI's National Counterintelligence Task Force?

From my interactions with the FBI and the NCITF, I understand that the principal purpose of the latter is to facilitate information sharing and interagency coordination supporting the FBI's counterintelligence (and related) activities, and to enhance threat awareness and security practices. A strategic CI program, under the leadership of the NCSC, would likely find the NCITF a useful resource.

NCSC's Duties, Authorities, and Resources

17. Which duties and activities are (or should be) an essential part of NCSC's mission?

The single most important duty of the Director NCSC is to head U.S. counterintelligence, not merely in name, but in fact, as contemplated by the CI Enhancement Act of 2002.

The current CI enterprise is built to support individual department and agency mission sets – all of which are vital. But it is not built to identify, assess, neutralize and exploit foreign intelligence operations directed against the United States. If we are ever to get ahead of the threat, the NCSC will need to lead the transformation of US counterintelligence to work as a coherent whole.

To that end, the head of U.S. counterintelligence should be designated the program manager of a statutory strategic CI program, and assigned funding and authorities to that end. Resources would include dedicated, country-specific strategic operational planning teams, drawn from across the CI community, and the authority to task select elements within the operational agencies for joint execution.

Threat prioritization, strategic guidance, budget assessments, training, education and public outreach, as itemized within the NCSC enabling statute, are all inherent duties of the office charged with leading and integrating the profession.

Whether or not the NCSC should retain responsibility for protective security is a more complicated question. To be sure, there is an inherent partnership between counterintelligence and the distributed functions of security, and a vital two-way flow of information. U.S. counterintelligence identifies foreign threats, and provides threat information to those responsible for protective security across the USG, as well as high priority private sector entities, so they may assess their risk and implement security plans and programs. Security managers in turn need to provide CI with incident reports and related information that may be indicators of foreign elicitation attempts, cyber penetrations, and the like.

But focusing the bulk of the NCSC's time and attention on security concerns, as has been the recent practice, is not the answer. One can pile on so much security that no one can move and still there will be a purposeful adversary looking for ways to get at what it wants. It falls to our CI agencies to defeat foreign intelligence services operating against the U.S. And that is why the core CI mission of the NCSC was and remains so important.

18. How should the Intelligence Community best conduct educational outreach to other U.S. government agencies and academic and private sector entities?

a. What role should NCSC play in educational outreach?

The NCSC has a leading role to play in educating the public about U.S. counterintelligence – what it is, what it does, and why, as well as coordinating foreign intelligence threat warnings.

b. How should NCSC coordinate with FBI and other U.S. government agencies to conduct outreach?

The FBI has long tasked its 56 field offices to identify and engage business, industry and academia at risk to foreign intelligence exploitation, in order to raise threat awareness and facilitate incident and other reporting back to the IC. The FBI should be keeping the NCSC fully and currently informed of these activities, and any insights they may provide.

c. Should NCSC develop a strategic plan to prioritize outreach efforts?

I do not know whether a strategic plan would be useful at this time, but I could envision the need to prioritize outreach if the IC/CI were to acquire relevant insights into foreign intelligence operations and collection targets requiring special attention.

19. The Committee understands that NCSC has not been consistently carrying out vulnerability assessments.

a. Why are such assessments important?

Effective security plans and programs are based on realistic risk assessments, which require an understanding of both threat and vulnerabilities.

b. What resources and authorities would NCSC need to conduct vulnerability assessments in compliance with statutory requirements?

As I read the statute, the NCSC has discretionary authority to conduct or coordinate such vulnerability assessments as it deems necessary or useful, subject to applicable law. Resource requirements would vary, depending on the type and quantity of vulnerability assessments planned. As an example from my time in office, we were instrumental in facilitating red-team testing of certain sensitive government facilities, drawing on funds allocated to those facilities for that purpose.

c. Rather than directly assessing the vulnerabilities of private sector and academic entities, should NCSC develop standards, criteria, and guidance for organizations in these sectors to do their own assessments?

In my view, the national-level office should provide policy and strategy guidance, but leave vulnerability assessments to those in the best position to perform them. Those who are in the field and know their business from the inside are far better equipped to identify vulnerabilities in their practices, personnel, physical plants, critical information and IT infrastructures. Moreover, potential vulnerabilities vary widely, depending on the business or industry or academic institution. Where standardized criteria or guidance may be useful for a given industry, I would defer to those government agencies charged with working directly with those sectors (e.g., DCSC and the defense contractor base; FDA and the pharmaceutical industry; etc.)

d. Should Congress require such entities to conduct vulnerability assessments and take reasonable steps to mitigate identified vulnerabilities?

In my opinion, private entities who enter into sensitive contractual or grant relationships with the federal government should be required to demonstrate due attention and care to mitigating vulnerabilities to foreign intelligence exploitation.

20. The Committee understands the NCSC has not been consistently coordinating counterintelligence research and development efforts.

a. Why is this important?

b. What resources and authorities would NCSC need to coordinate counterintelligence research and development efforts in compliance with statutory requirements?

To my knowledge, there is no dedicated R&D effort to support the work of U.S. counterintelligence – but there should be. Doubtless there are many ways in which the tradecraft of counterintelligence, and its various analytic and operational tools, could be enhanced through the creative exploitation and application of new technologies. The Defense Science Board (DSB) looked at this issue in 2019, and recommended that the Undersecretary for Intelligence and the Undersecretary for Research and Engineering jointly explore ways to exploit existing S&T investments to improve DoD's counterintelligence capabilities and tools, including:

- Establishing an effort within the office of the Secretary of Defense, perhaps including support from a University Affiliated Research Center or a Federally Funded R&D Center, dedicated to examining new technologies which could enhance the CI mission within the DoD; and
- Creating a program, plan, and budget to accommodate the continuous infusion of these technologies into CI operations.

I would urge the Committee to follow up directly with the office of the Secretary of Defense on the status of this DSB recommendation.

21. In which key areas is NCSC under-resourced for its mission?

The current complement of duties and billets at the NCSC appear to be heavily skewed in support of its security-related responsibilities, with far less effort devoted to counterintelligence. As a result, I fear the original purpose for which the NCSC was created has been neglected. A revalidation of that core CI mission, as discussed above, should drive a realignment of resources to support national CI objectives.

Having served as the first head of U.S. counterintelligence, charged with setting up the office of the (now) NCSC, I am not in favor of big new bureaucratic structures that take people away from the field. However, as part of the strategic CI program, I strongly recommend that an elite national CI operations center, manned and empowered by the constituent members of the CI community, be established at the NCSC to integrate and orchestrate operational and analytic activities across the CI community to strategic effect.

In my view, the greater obstacle to progress is not so much lack of resources as it is the mixed signals over the core mission of the national CI office. There is an urgent need to clear up that confusion, if U.S. counterintelligence is ever to have the cohesion needed to get ahead of the threat. Establishing in law a strategic CI program, and reaffirming the responsibility of the head of U.S. counterintelligence to lead that effort, are vital first steps.

22. What resources and authorities does NCSC need to better influence the counterintelligence budgets of its entities?

Under the current business model, with program and budgeting authorities divided among the departments and agencies, we are getting about the best we can expect out of our CI programs. For the future, avoiding strategic CI failure will require more than simply doing more of the same. Without the power of a common purse, however, the mission of integrating and redirecting U.S. counterintelligence to achieve strategic cohesion may well be impossible.

To that end, the Director of National Intelligence should delegate his directive authority over CI budget, analysis, collection and other operations, to the NCSC, which would go a long way toward investing the national CI office with the authorities and resources it must have to succeed.

I know that departments and agencies jealously guard their power over their own purse and operations, and for good reason. So let me be clear. In my view, the NCSC does not need plenary directive authority over all CI budgets and programs. Those matters that are properly the purview of the individual CI missions assigned to the operational components must remain under their control (and accountability). The NCSC should review and advise the DNI on the whole of the CI enterprise, which can be accomplished as part of the overall NIP budget preparation.

However, the NSCS does need directive authority over the elements of the strategic counterintelligence program, distributed among the several operational components. While tactical execution must remain with the responsible agencies, D/NCSC should serve as program manager for strategic counterintelligence, with dedicated resources at the national level and as assigned among the executing departments and agencies, to identify, assess, neutralize and exploit high priority foreign intelligence threats to the United States. This should include an effective means of holding agencies accountable for meeting national objectives that go beyond their individual missions.

23. Should Congress establish a separate appropriation for NCSC to support non-IC U.S. government agencies and counterintelligence programs that support strategic objectives?

No. Adversary intelligence services do not target the Commerce Department, or DoE laboratories, or the U.S. Congress; they target the United States. Our counterintelligence enterprise must be equally strategic in its orientation and response.

Unfortunately, U.S. counterintelligence is not currently configured to work as a strategic whole; rather, each of the lead agencies has a separate CI mission that grew up as part of their larger responsibilities, with no overarching structure to unite them. The tactical focus of U.S. counterintelligence professionals – our clandestine HUMINT collectors, military commanders responsible for force protection, or law enforcement officers pursuing espionage leads -- is vital to

individual mission success, but they do not answer the larger questions: What are the threats to America's national and economic security presented by foreign intelligence adversaries and what should we do about them?

The Director NCSC should be designated program manager of a strategic IC program, to provide the structure, processes and centralized orchestration needed to go on the offense against foreign intelligence threats wherever they are directed against the United States or our vital interests. As a baseline, CI agencies should designate strategic CI units from among their existing capabilities, or identify such additional capabilities as they may need to support and carry out this new national CI mission. The Committee may want to task the Director NCSC to gather and assess these funding requirements as part of the ODNI budget submission to the Congress.

NCSC's Structure

24. What are the key benefits and drawbacks of remaining a Center within ODNI? [and]

25. What is the ideal organization and location for NCSC to best counter the current foreign intelligence threat landscape?

- **a. Should NCSC remain exclusively within the Intelligence Community, or should it acquire non-title 50 authorities as well, given its current focus on outreach and engagement with non-IC entities?**
- **b. Should NCSC become an independent National Counterintelligence and Security Agency?**

I believe there is a strong argument for splitting national level policy and oversight of security and counterintelligence into two parts, under two separate entities.

1. A security center, outside the intelligence community, could be established to advance, coordinate, and hold agencies accountable for security plans and programs across the federal government, and to interface with the private sector. It would also serve as public spokesman for threat awareness and best practices, which span not only foreign intelligence threats but the full range of cyber threats (including criminal activities), supply chain integrity, and insider concerns (leaks, disgruntled employees), in coordination with sister agencies (*e.g.* CISA, DCSA).

2. The (smaller) national CI office would remain within the ODNI as a separate entity. Counterintelligence is by its very name, definition, authorities and practices an intelligence mission. It is executed by the designated operating agencies. They need a leader to provide strategic cohesion, as the 2002 Counterintelligence Enhancement Act originally provided, and to perform the duties outlined in that law (threat prioritization, national strategy, budget oversight, training and education).

   To that end, the national head of U.S. counterintelligence needs to be empowered to serve as program director of a new strategic CI program, including authority over select (new?) resources across the CI community dedicated to that program. The national office would keep book on foreign intelligence threats, array blue side capabilities against them, develop strategic operational plans to neutralize or exploit those threats, and coordinate their execution. As I

emphasized in my testimony, this is a straightforward offensive capability that the United States does not have but sorely needs.

No one wants to see the bureaucracy grow any bigger than it already is; but in this case, I think that two entities would actually prove more efficient:

- A security center, outside the IC, would have the clarity of purpose needed to align responsibilities and staffing with security disciplines across the government and the private sector, and get to work.
- The same is true of a national CI office, which by contrast would be manned by analysts and strategic planning team members from across the IC/CI community to work strategic CI targets. The office would not serve as another "czar" – which we do not need -- but an actual new national-level capability, which would accrue to the benefit of our CI agencies across the board.

Each center would know the parameters of their mission; staffing requirements would not be any greater but they would be easier to meet (with security outside the IC); and each would have a clear and vital job to perform. In my opinion, conflating security and counterintelligence national offices, as they are now, is not saving money or resources; it is just inviting confusion and wasting precious time and effort – all to the benefit of our adversaries.

Questions for the Record
U.S. Senate Select Committee on Intelligence
Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center
Open Session
September 21, 2022

[From Senator Feinstein]

The U.S. Counterintelligence Enterprise

- **Which legal responsibilities should non-IC entities—including U.S. government agencies, academic institutions, and private sector companies—have to protect their intellectual property, research, technologies, and data with national security implications?**

  Academic institutions should have a legal responsibility to establish a policy that mandates the highest standards of integrity and compliance in ensuring the security of their member's research portfolios. This policy should establish the framework for (a) establishing a Research Security Office (RSO) as the responsible office for classified information, controlled unclassified information, management of the system's secure computing enclave, foreign influence reporting, and export controls, (b) achieving the highest level of compliance with applicable ethical, legal, regulatory, contractual and system standards and requirements in securing research portfolios, (c) promoting an organizational culture of compliance in meeting federal requirements to maintain federal funding, and (d) assisting members in related compliance operations.

- **Which incentives and resources could Congress provide to help non-Intelligence Community entities better protect their intellectual property, research, technologies, and data from foreign adversaries?**

  The CHIPS and Science Act (P.L. 117-167) authorizes the establishment of a research security and integrity information-sharing analysis organization (section 10338) and a regional secure computing enclave pilot program (section 10374(d)). Congress should appropriate funding to the National Science Foundation to establish these programs, in partnership with institutions of higher education with solid research security track records, to help academic institutions protect their intellectual capital, research, technologies, and data from foreign adversaries.

  Both initiatives would increase the ability of universities to collaborate more effectively regionally and nationally. They would also help to provide more limited, less well-resourced universities access to significant new capabilities for securing the research enterprise.

- **What are the biggest challenges academic entities face in confronting foreign adversarial intelligence collection and economic espionage?**

  The US higher education system operates under a unique set of principles and commitments fundamental to the academy. Any attempt to secure the research enterprise must not compromise these principles, which include:

- Openness and transparency
- Accountability and honesty
- Impartiality and objectivity
- Respect
- Freedom of inquiry
- Reciprocity
- Merit-based competition

While these foundational principles are our greatest strengths, they can also present some of our most significant vulnerabilities, and therein lies the challenge. For example, our culture of openness can lead to potentially more substantial exposure to malign actors and risk. Our desire to collaborate with the brightest minds in the world might enhance the capabilities of some who do not share our fundamental values and national interests. Our world-class laboratories and equipment can provide access to world-class laboratories and equipment unavailable in most other countries. While this access can help solve the world's most challenging problems, it can also give greater exposure to risk. Our focus on pushing science to its limits can provide access to cutting-edge technology and scientific processes that others seek to emulate or acquire. Once again, this is not without some risk. Finally, institutional autonomy and academic freedom can make internal coordination difficult.

Each of these strengths makes our research enterprise effective and robust. As we implement measures to address risk in our institutions, we must ensure our solutions don't negatively impact our strengths. The challenge is how we achieve the proper balance.

- **Given the generally lawful nature of foreign acquisition of U.S. technology, does Congress need to consider additional updates to the Committee on Foreign Investment in the United States (CFIUS) to address the remaining loopholes?**

  The Committee on Foreign Investment in the United States (CFIUS) provisions are outside my area of expertise, so I cannot answer this question.

- **How can the U.S. government best strike a balance between protecting national security and preserving a culture of international collaboration, free enterprise, and open research?**

  One of the primary roles of academic institutions is the free and open generation and dissemination of knowledge. Known for its open and collaborative nature, the US research enterprise provides the foundation for a diverse and driven workforce, fostering discovery and innovation. International collaboration is crucial to scientific advancement and the success of research institutions in the United States.

  American universities have become a magnet for students and researchers worldwide to join forces in solving our nation's most pressing problems and promoting scientific advancement. Unfortunately, we are not playing on a level playing field. Our technological leadership is under siege from countries like Russia, China, Iran, and others whose rules for information sharing and research integrity differ from ours. These countries are extracting intellectual capital, cutting-edge data, and technical expertise at an unprecedented rate and putting our technological leadership at risk. Academic sector entities must work closely with our federal partners to protect information and research with national security implications. To be most

effective, integration and information sharing between the research security community and the U.S. counterintelligence enterprise must be seamless.

- **What can be done to enhance U.S. government agencies' ability to conduct investigations into grant fraud and technology transfer in collaboration with universities?**

  Robust relationships with our Federal partners and open exchange of information have been critical to our efforts to ensure the integrity and security of Federal grant funding awarded to Texas A&M System entities. When we learn of issues affecting our grant awards, we quickly report them to the appropriate Federal entity and take seriously any issues highlighted for us by our Federal partners.

- **To what extent should the State Department vet international students, professors, or employees from a counterintelligence perspective?**

  Understanding our collaborators is one of the most important aspects of any research security program. The Texas A&M University System's Research Security Office has established a robust open-source due diligence program through which we review all visiting scholars and post-doctoral researchers from countries of concern, all personnel engaging in our work with Army Futures Command, the University Consortium for Applied Hypersonics, and our national laboratory efforts, and others based on risk.

  Additional support, in the form of open-source information sharing or vetting information, from the Federal government would be welcome.

- **Should academic institutions do their research security vetting of visiting students, professors, and employees?**

  - **What tools, resources, and support from the IC would be needed?**

  As noted above, The Texas A&M University System's Research Security Office has established a robust open-source due diligence program, which we believe should be a model for academia. Institutions that cannot develop a research security/due diligence program like the A&M System would benefit from a federally funded regional due diligence program launched in partnership with an academic institution through which universities could seek assistance.

  We have developed several tools that allow us to scour open-source information more efficiently and effectively as part of our due diligence efforts. These tools have significantly decreased the time and staffing required to perform adequate due diligence. With minimal funding, these tools could be further developed and provided to other institutions to enhance due diligence capabilities.

- **How can the U.S. government, in general, and the Intelligence Community, in particular, better communicate the foreign intelligence threat to the American public, private sector companies, and academic institutions?**

To effectively communicate the foreign intelligence threat, the U.S. government, generally, and Intelligence Community, in particular, must work to understand the U.S. research enterprise and form partnerships with academic institutions. One cannot simply strike and replace industry for academia in bulletins and messaging – they are not the same. Messages must be tailored to the audience to have the most significant effect.

The ability to share actionable open-source information is also critical. While classified intelligence has its place, universities generally need access to UNCLASSIFIED, open-source information for their research security efforts. This allows for the broadest dissemination of threat information.

Clear communication channels between universities and their federal partners are also critical. The Texas A&M University System's Research Security Office is the single point of contact with Federal partners to exchange information related to threats from malign foreign actors. The RSO is a trusted member of the A&M research community and is in the best position to share relevant threat information with faculty and staff.

- **How can the U.S. government in general and the Intelligence Community in particular partner with non-Intelligence Community entities to prevent foreign intelligence penetration and exploitation?**

Key to our engagement with our federal partners has been the establishment of the Academic Security and Counter Exploitation (ASCE) working group, an association of university research professionals and their federal counterparts, which exists to leverage the expertise of universities that have demonstrated excellence in research security programs to help address the threat foreign adversaries pose to U.S. academic institutions.

The ASCE Executive Committee includes representatives from the FBI, DOD, State Department, and Commerce Department and meets bi-weekly to discuss threats to research security and mechanisms to combat them. The group works collaboratively to develop and share information on best practices for a successful research security program. ASCE also distributes a weekly Open-Source Media Summary to more than 3000 individuals from more than 300 academic institutions, government agencies, and cleared industries with ties to academia. Finally, ASCE hosts a four-day training seminar annually focused on securing the research enterprise. Now in its seventh year, the ASCE Seminar draws over 500 participants from academia, government, and industry each year.

- **Texas A&M has one of the most well-respected research security programs in academia.**

  - **What is unique about this program?**

First, the level of support we receive from the highest levels of the A&M System is exceptional. Chancellor John Sharp has stated publicly, "No one in higher education takes security as seriously as we do at The Texas A&M University System…and [we make] counterintelligence a priority, we intend to be a leader in protecting national interests and the sensitive work the Texas A&M System does in service to our country." With that kind of support from the top, it is easy to develop an exceptional research security program that is well-respected within academia.

Secondly, we have organized for success. We created a Research Security Office in 2016 and tasked it with oversight of the research security efforts for the 11 universities and eight state agencies that comprise the A&M System. A Chief Research Security Officer at the associate vice-chancellor level leads that office. The Chief Research Security Officer has extensive government and academic experience and holds a Ph.D. and credentials in industrial security.

The research security office oversees our classified research programs, our controlled unclassified information management, and our export control program. Our ability to manage these three overlapping programs from a single office provides excellent synergy and enhances effectiveness. The research security office has also developed an effective working relationship with compliance offices across the A&M System to provide unity of command and unity of effort in our mission to secure our research enterprise.

Texas A&M University System Policy designates the Chief Research Security Officer as the A&M System's single point of contact with federal partners engaging the A&M System on research security matters. This policy has resulted in more effective communication between the A&M System, its members, and our federal partners.

Thirdly, the A&M System developed a secure computing enclave in 2016 that allows us to secure federally funded research outside the wider A&M System networks. This secure computing enclave meets all the requisite NIST 800-171 requirements for protecting federal information on non-federal systems. We are also deploying a secure Microsoft® Government Cloud environment in which most of our large federally-funded programs will operate in the future.

Finally, we have chosen to take a leadership role in the national effort to secure our research enterprise. We established the Academic Security and Counter-Exploitation Program in 2017 to collaborate with other universities on this effort. The group has now grown to over 200 participating universities. We have published a weekly Open-Source Media Summary (OSMS) distributed to the academic community and our federal partners weekly at no cost. The OSMS provides timely threat information explicitly focused on the academic community. We also host an annual training that brings the academic community and its federal partners together to benchmark, share information, network, and move the effort for securing our research enterprise forward.

In short, the A&M System's research security program is unique because we have exceptional buy-in and leadership from the top down. We chose to act early, implementing the first research security office and establishing the first Chief Research Security Officer position in

academia. The A&M System implemented the requirements for NSPM-33 in 2016. Our program is also unique because we saw the need and chose to lead the research security effort in academia more than five years ago. We remain committed to that effort today.

- **How does Texas A&M assess the return on investment from its research security program?**

It isn't easy to put a price on our national security. We choose not to measure our research security investments in terms of profits and losses. The ultimate measure is how effectively we protect the federal research dollars we have been entrusted with and how our research contributes to the overall national-security effort. With that said, our research security effort has been designed for efficiency and effectiveness. The fact that our research security efforts have been recognized on a national level four times over the last six years by the Defense Counterintelligence and Security Agency suggests that our investments are paying high dividends in our ability to secure the research enterprise and contribute to our national defense.

- **To what extent has Texas A&M shared lessons learned with other academic institutions?**

As noted previously, the A&M System established the Academic Security and Counter Exploitation Program as a mechanism to leverage the expertise of universities with demonstrated excellence in research security programs to help address the threat that malign foreign actors pose to U.S. academic institutions.

We established the first Academic Security and Counter Exploitation Training Seminar in 2015 to provide a forum for those academic institutions participating in the NISP to benchmark and share best practices from their respective programs. The conference has grown since that first year to include the broader academic community and increased federal engagement from the FBI, DOJ, DOD, NSF, NIH, Office of the Director of National Intelligence, and Office of Science and Technology Policy. We were honored to have Chairman Warner and Senator Cornyn join the conference in 2021 to talk about the threat and the work you're doing here in Congress. We're well on our way in planning for next year's conference, which will be held in College Station from March 6-10, 2023. This year's seminar will have an international component for the first time resulting from our partnership with the Department of State.

While the Academic Security and Counter Exploitation Training Seminar provides an opportunity for academic security professionals to come together physically once a year, we have also developed ongoing platforms for virtual collaboration. We created a listserv for security professionals in academia to seek advice, benchmark, and share best practices daily. The listserv currently has over 200 member universities and 3000 individual participants and remains highly active.

We also share a weekly ASCE Open-Source Media Summary to share information with academia. We are pleased to reach over 3000 readers each week across academia, the private sector, and the Federal government, including from Capitol Hill.

- **Can you explain how university participation in efforts such as the Academic Security Conference helps those universities with less experience in research security address foreign influence threats such as foreign government-sponsored talent recruitment programs?**

As noted above, ASCE serves as a mechanism for universities, regardless of their level of research security experience, to collaborate and share information – both in person annually and virtually as often as desired – on threats they are seeing and best practices to address them.

The OSMS provides weekly actionable information on threats to the academic research enterprise directly to those individuals within the academic community who can address the threats. The OSMS also provides our federal partners with insight into the academic community's unique aspects so that they can better communicate the danger.

The annual ASCE Seminar provides an opportunity for academic security professionals to come together physically once a year with federal law enforcement agencies, research security policymakers, and leaders from government and academia to learn techniques for securing the research enterprise, benchmark, network, and collaborate.

- **What trends have you observed in the types of university research targeted by foreign governments in recent years?**

My observations tell me our adversaries cast a wide net in their efforts to access our technology. The focus is not solely on sensitive or proprietary research and technology. They are after fundamental research to facilitate their ability to leapfrog in the research process. Consequently, our efforts should have a wide aperture as well.

One very positive trend I see daily is the academy's progress in understanding, accepting, and addressing the research security threat over the past five years. The danger facing university professors, students, and institutions from malign foreign actors and foreign intelligence is widely understood and accepted today. Still, work remains to improve security and transparency across the research enterprise to allow us to continue operating in an open and collaborative environment on the international stage.

Questions for the Record
U.S. Senate Select Committee on Intelligence
Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center
Open Session
September 21, 2022

Robert Sheldon
Director, Public Policy & Strategy

[From Senator Feinstein]

The U.S. Counterintelligence Enterprise

1. **Which legal responsibilities should non-IC entities—including U.S. government agencies, academic institutions, and private sector companies—have to protect their intellectual property, research, technologies, and data with national security implications?**

There is no single, uniform data protection scheme for national-security relevant information. Laws, regulations, contracts, and customer commitments or expectations can each apply particular requirements, depending on the context. This system does create the potential for gaps or overlaps. However, a singular approach to protecting national-security relevant information may also carry risks. These include impacts to the pace of cross-functional research, research in areas with dual-use implications, and innovation generally. Where the U.S. government issues specific guidance, such as threat advisories, to sectors or organizations then it is important to advise on how to mitigate such threats and to empower them with the appropriate tools to do so where they may not exist.

2. **Which incentives and resources could Congress provide to help non-Intelligence Community entities better protect their intellectual property, research, technologies, and data from foreign adversaries?**

Two lines of effort could help organizations become better informed about threats and take steps to stop them. (A) The U.S. national security enterprise should more clearly communicate areas of research/technology with perceived national security implications. Proactive disclosures about emerging intelligence collection requirements from foreign adversaries would help inform the threat model used by entities working in those areas. (B) From a cybersecurity standpoint, targeted efforts to increase defenses by small- and medium-sized entities could be impactful. To this end, as noted in my testimony, Congress could take steps to increase national incident response capacity and explore tax-mechanisms to promote and enhance adoption of comprehensive cybersecurity solutions.

3. **What are the biggest challenges private sector entities face in confronting foreign adversarial intelligence collection and economic espionage?**

While private sector entities face an array of threats that range from problematic investors to malicious insiders, cybersecurity remains the central challenge. Even entities that follow all current, applicable cybersecurity controls and best practices will be breached periodically by capable adversaries. To successfully face these challenges, organizations must continuously improve their cybersecurity posture, adopt zero trust principles, and proactively hunt threats within their networks. Organizations should strongly consider leveraging managed security services providers to operate with the speed necessary to defeat threats.

4. **Given the generally lawful nature of foreign acquisition of U.S. technology, does Congress need to consider additional updates to the Committee on Foreign Investment in the United States (CFIUS) to address remaining loopholes?**

While my co-panelists are better situated to address CFIUS-related questions, I'll make two minor observations. First, given macroeconomic conditions, it is reasonable to assume an increased rate of M&A activity across the technology and startup ecosystem over the coming years. Second, in addition to broad transaction-related risks, CrowdStrike has observed threat actors specifically targeting entities engaged in the M&A process.

5. **How can the U.S. government best strike a balance between protecting national security and preserving a culture of international collaboration, free enterprise, and open research?**

While my co-panelists are better situated to address this question, I note that a key step is the potential to exacerbate potential tensions between these aims with insufficiently nuanced policy. Continuing the Committee's approach to engaging stakeholders from different backgrounds and with different perspectives is key, as is broadening outreach to different parts of industry.

6. **To what extent should the State Department vet foreign students, professors, or employees from a counterintelligence perspective?**

Whether an individual is from a foreign country may not warrant additional scrutiny on its own. Instead, to the extent that additional vetting is required, it should be risk-informed, consistent, fair, and account for differences between these stakeholder groups. Like with positions of trust, a totality of circumstances may warrant additional scrutiny. For example, a student from one country studying at a liberal arts university may merit a different process than an employee from a country with a targeted espionage apparatus working in a lab supported by U.S. government funding for defense-relevant research.

7. **How can the U.S. government in general and the Intelligence Community in particular better communicate the foreign intelligence threat to the American public, private sector companies, and academic institutions?**

As noted above (in Answer 2(A)), the Government and Intelligence Community can help identify new targets or trends in foreign intelligence collection priorities. In some instances, broad communications about these developments may be appropriate. In other instances, the government can provide more clarity–and reach scale–by working through trusted entities with more expansive commercial relationships. To these ends, models like CISA's Joint Cyber Defense Collaborate (JCDC) merit continued experimentation and investment.

8. **How can the U.S. government in general and the Intelligence Community in particular partner with non-Intelligence Community entities to prevent foreign intelligence penetration and exploitation?**

As noted above, from an industry engagement perspective, policymakers should explore broadening access to cybersecurity capabilities and increase incident response capacity (Answer 2) and explore greater use of JCDC and similar mechanisms (Answer 7).

Further, the U.S. should use all mechanisms at its disposal, including industry engagement where appropriate and additive, to degrade threat actors' ability to effectuate malicious cyber activity. This includes cooperative efforts to directly target malicious infrastructure.

9. **CrowdStrike is a recognized leader in cybersecurity.**

    a. **From your perspective, what role should commercial providers play in defending academic institutions and private sector entities from foreign intelligence entity cyber attacks?**

The private sector is on the "front lines" combating cyber threats. Government entities can and should help communicate new threats and coordinate response efforts, as well as reduce the overall threat environment (e.g., as described in Answer 8). But commercial providers perform the actual defense, and in virtually all cases also perform response and remediation in response to incidents. From a roles and missions standpoint, this division of labor is appropriate given each entities' respective authorities, missions, resources, and capabilities. The central policy questions relate to how each entity can perform their missions better, with more efficiency, and at greater scale.

    b. **How can commercial cybersecurity providers such as CrowdStrike better partner with the U.S. government to defend non-Intelligence Community entities from foreign cyber attacks?**

The U.S. government, particularly the nation's lead federal agency for the protection of critical infrastructure, the Cybersecurity and Infrastructure Security Agency (CISA) does not have the cyber incident response capacity needed to respond to broad-based, concurrent significant cyber incidents impacting critical infrastructure entities or the federal government.

As a community, we should undertake a more serious conversation about expanding national Incident Response (IR) capacity. IR demand is incredibly elastic, and IR supply is relatively fixed. A program that retained skilled providers in advance for use during significant cyber incidents could expand the cybersecurity workforce and strengthen national resilience. Such a program would ensure skilled providers are standing ready to offer assistance within a stipulated time frame, and under other terms outlined in a Service Level Agreement (SLA).

Eligibility for benefits under such a program would likely be based on need or vulnerability (e.g., for small businesses), and/or on criticality (e.g, entities with a national security nexus or critical infrastructure entities with systemic importance), in accordance with CISA's judgment.

c. What role, if any, should U.S. government entities such as CYBERCOM play in defending non-U.S. government entities from foreign cyber attacks?

Please see Answer 8.

d. What statutory or policy changes, if any, are necessary to clarify and strengthen the relationship between commercial cybersecurity providers and the U.S. government?

The current balance of responsibilities between commercial cybersecurity providers and various government agencies is the result of several decades of iteration, experimentation, stress-tests, case law, etc. Like other complex policy areas, outcomes are far from perfect. But the fundamental roles and missions of each sector (described in Answer 9a) are sound. Each sector should continue to develop its capacity to meet evolving threats (see Answer 2), and each sector should work together in a more integrated way (see Answer 7).

###