INNOVATION NATION: LEVERAGING TECHNOLOGY TO SECURE CYBER SPACE AND STREAMLINE COMPLIANCE

FIELD HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MAY 28, 2025

Serial No. 119–17

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE
61–340 WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas, *Vice Chair*
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona
ANDREW OGLES, Tennessee
SHERI BIGGS, South Carolina
GABE EVANS, Colorado
RYAN MACKENZIE, Pennsylvania
BRAD KNOTT, North Carolina

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
ERIC SWALWELL, California
J. LUIS CORREA, California
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
DANIEL S. GOLDMAN, New York
DELIA C. RAMIREZ, Illinois
TIMOTHY M. KENNEDY, New York
LAMONICA MCIVER, New Jersey
JULIE JOHNSON, Texas, *Vice Ranking Member*
PABLO JOSÉ HERNÁNDEZ, Puerto Rico
NELLIE POU, New Jersey
TROY A. CARTER, Louisiana
ROBERT GARCIA, California
AL GREEN, Texas

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

CONTENTS

INNOVATION NATION: LEVERAGING TECHNOLOGY TO SECURE CYBER SPACE AND STREAMLINE COMPLIANCE

Wednesday, May 28, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
STANFORD, CA.

The committee met, pursuant to notice, at 2 p.m., at Stanford University, George P. Schultz Building, 426 Galvez Mall, Stanford, California, Hon. Mark E. Green (Chairman of the committee) presiding.

Present: Representatives Green, Garbarino, and Swalwell.

Chairman GREEN. The Committee on Homeland Security will come to order.

Without objection the Chair may declare the committee in recess at any point.

Today's field hearing will explore how the public and private sectors can work together to address the economic models of cybersecurity. To do this, we will examine the cyber threat landscape, cyber regulations and the technology that will improve America's cybersecurity posture.

I want to thank the Members of the committee who made it out for this and took time to join us here in Silicon Valley.

I now recognize myself for an opening statement.

Well, good afternoon, and I want to thank all of you for coming today. The topic is one that is incredibly important for our country, and I thank the Hoover Institution for hosting this on such an incredibly beautiful campus.

I do not know who brought the weather here. Is it like this all the time? I mean, it is incredible.

It is not a coincidence that we are holding today's hearing here in the middle of Silicon Valley. Since World War II Silicon Valley has been the world's shining example of what a Nation can accomplish when innovation is unleashed.

It is the home of some of America's most talented and creative minds, innovators who are spearheading major breakthroughs in technological development. From semiconductors to social media, Silicon Valley has produced innovations that have changed the way we work, communicate, and complete daily tasks.

As we know, great technological advancements come with great responsibility. I am here today to emphasize the importance of prioritizing our cybersecurity as we build new capabilities that will continue to change the world.

I have prioritized cybersecurity for myself in this Congress and for the Committee on Homeland Security, and I hope industry partners that are here and across the country will join us in this mission to improve our cyber resilience against nation-states as well as criminal actors, strengthen our offensive posture, and develop new capabilities that incorporate security from the start.

I strongly believe that allowing American innovation to flourish is critical to strengthening our national security. That is why we must start by injecting common sense into the regulatory regime. The increasingly burdensome, costly, and duplicative requirements placed on our innovators are stifling our innovation and hindering our national security.

Instead we must continue to explore technological solutions for regulatory compliance and ways that we, as Congress, can help deconflict and simplify cyber regulations.

This priority pairs well with another focus of mine in this Congress: changing the economic models of cybersecurity. The costs and incentives associated with cybersecurity are currently imbalanced in favor of the attacker rather than defender.

According to a report by IBM, the global average cost of a data breach in 2024 was nearly $4.9 million. In many cases, to inflict multimillion dollar damage on U.S. businesses, attackers only need some degree of technical knowledge and a laptop, a fraction of the cost faced by their victims.

Fixing the economic models of cybersecurity will require a concentrated effort across industry and our Government. First, we must raise the cost of cyber attacks for our adversaries. From strengthening our offensive posture in cyber space to creating innovative cybersecurity solutions, the United States must make it more challenging and costly for adversaries to strike.

Second, we must ensure that American businesses, especially private owners and operators of critical infrastructure, are investing heavily in cybersecurity. There needs to be a greater demand for products designed with cybersecurity in mind, accompanied by a supply shift toward more secure information technology and operational technology.

There is an indisputable connection between what happens here in Silicon Valley and the security of U.S. critical infrastructure. The technology and cybersecurity solutions produced here have applications across all critical infrastructure sectors.

By improving investment in cybersecurity and raising costs for our adversaries, the entire Nation will be more secure.

Cybersecurity truly is a team sport. Our collective defense against cyber threats relies upon private-public partnerships and information sharing. We want to turn that information sharing into action.

I am grateful for Chairman Garbarino's efforts to preserve and enhance these partnerships, including through the reauthorization of CISA 2015, and I look forward to discussing other ways to strengthen public-private partnerships in cybersecurity.

I want to thank our witnesses for joining us today. I look forward to discussing the current threat landscape with each of you and to examining ways we can realign the economic models of cybersecurity.

Our discussion will position us well to delve into finding solutions with some of our Nation's most prominent innovators during the breakout session that follows this hearing.

We have much more work to get done and to get to where we need to be, but I am confident that if we work toward these objectives together, we will accomplish our mission. I look forward to the effort.

[The statement of Chairman Green follows:]

STATEMENT OF CHAIRMAN MARK E. GREEN, MD

MAY 28, 2025

Good afternoon everyone. Thank you to The Hoover Institution for hosting us on this beautiful campus.

It is no coincidence that we are holding today's hearing in the heart of Silicon Valley. Since World War II, Silicon Valley has been the world's shining example of what a nation can accomplish when innovation is unleashed. It is home to some of America's most talented and creative minds—innovators who are spearheading major breakthroughs in technological development. From semiconductors to social media, Silicon Valley has produced innovations that have changed the way we work, communicate, and complete daily tasks.

As we know, great technological advancements come with great responsibilities. I am here today to emphasize the importance of prioritizing cybersecurity as we build new capabilities that will continue to change the world. I have prioritized cybersecurity in Congress, and I hope industry partners—many of which are headquartered here—will join me in our mission to improve our cyber resilience against nation-state and criminal actors, strengthen our offensive posture, and develop new capabilities that incorporate security from the start.

I strongly believe that allowing American innovation to flourish is critical to strengthening our national security. That's why we must start by injecting common sense into the regulatory regime. The increasingly burdensome, costly, and duplicative requirements placed on our innovators are stifling our innovation and hindering our national security.

Instead, we must continue to explore technological solutions for regulatory compliance and ways that we, as a Congress, can help deconflict and simplify cyber regulations.

This priority pairs well with another focus of mine this Congress: changing the economic models of cybersecurity. The costs and incentives associated with cybersecurity are currently imbalanced in favor of attackers, rather than defenders.

According to a report by IBM, the global average cost of a data breach in 2024 was nearly $4.9 million. In many cases, to inflict multi-million-dollar damage on U.S. businesses, attackers only need some degree of technical knowledge and a laptop—a fraction of the costs faced by their victims.

Fixing the economic models of cybersecurity will require a concerted effort across industry and Government. First, we must raise the cost of cyber attacks for our adversaries. From strengthening our offensive posture in cyber space to creating innovative cybersecurity solutions, the United States must make it more challenging and costly for adversaries to strike.

Second, we must ensure that American businesses—especially private owners and operators of critical infrastructure—are investing in cybersecurity. There needs to be a greater demand for products designed with cybersecurity in mind, accompanied by a supply shift toward more secure information technology and operational technology.

There is an undisputable connection between what happens here in Silicon Valley and the security of U.S. critical infrastructure. The technology and cybersecurity solutions produced here have applications across all critical infrastructure sectors.

By improving investment in cybersecurity and raising costs for our adversaries, the entire Nation will be more secure.

Cybersecurity truly is a team sport. Our collective defense against cyber threats relies upon public-private partnerships and information sharing. I'm grateful for Chairman Garbarino's efforts to preserve and enhance these partnerships, including through the reauthorization of CISA 2015, and I look forward to discussing other ways to strengthen public-private partnerships in cybersecurity.

I want to thank our witnesses for joining us here in Silicon Valley. I look forward to discussing the current threat landscape with you, and to examining ways we can

realign the economic models of cybersecurity. Our discussion will position us well to delve into finding solutions with some of our Nation's most prominent innovators during the breakout session following this hearing.

We have much work to do to get to where we need to be, but I am confident that if we work toward those objectives together, we can get there. I look forward to the effort.

Chairman GREEN. I would now like to recognize the Chairman of the Subcommittee on Cybersecurity and Homeland Security Committee, Mr. Garbarino from New York.

Mr. GARBARINO. Thank you, Mr. Chairman. Thank you very much for having this hearing.

Good afternoon, everyone. I am honored to join our Nation's innovators today here in Silicon Valley. Thank you for your interest in our hearing and your partnership.

Our enemies aggressively target U.S. critical infrastructure through novel techniques and persistent campaigns. Volt and Salt Typhoon, 2 China-backed threat actors, demonstrate that America's foreign adversaries are intent on finding opportunities to exploit our cybersecurity weaknesses wherever they can. It is therefore crucial that America's cybersecurity capabilities remain ahead of our adversaries.

Bolstering cybersecurity resilience requires a whole-of-society approach, one that unlocks full potential of our innovative capacity to address and prevent vulnerabilities in our IT and OT.

The companies here in Silicon Valley are often on the front lines of cybersecurity defense, and they will help develop solutions to bolster our ability to counter these threats.

Ensuring we develop and use the right cybersecurity solutions requires a strong partnership between the public and private sectors.

The foundation of this collaboration is information sharing, a key focus for my subcommittee this Congress. Information sharing between the public and private sectors is beneficial not only for staying ahead of threat actors, but also for driving innovation to where it is needed most.

By sharing information about emerging threats and empowering CISA to manage cross-sectoral relationships, information sharing will help develop the tools we need to understand how threat actors operate in cyber space.

Innovation plays a critical role in keeping up with new tactics, techniques, and procedures of our adversaries in an increasingly active threat environment.

As part of our continued prioritization of information sharing, my subcommittee recently held a hearing on an important authority, the Cybersecurity Information Sharing Act of 2015, otherwise known as CISA 2015.

Information sharing between the public and private sectors heavily relies upon this Act. So it is imperative that Congress reauthorizes CISA 2015 before it expires later this year.

I was encouraged by Secretary Noem's statements in support of reauthorizing CISA 2015, when she came before the full committee just a few weeks ago and look forward to working with the administration to do so in the coming months.

Regulatory harmonization is another important topic that we will discuss during today's hearing. This is a topic which my subcommittee has explored extensively, especially in the context of

CIRCIA, the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

Industry's feedback is critical to obtain an effective, final rule that meets Congressional intent, which is why I look forward to hearing your perspectives on the current regulatory landscape.

I am also aware of the importance of providing for an ex parte process as rulemaking moves forward. This is something Secretary Noem has committed to providing, which will hopefully help remedy the rule's current shortfalls.

Our expert panelists have led the charge in protecting the United States from threats to our cybersecurity. I look forward to hearing your insights into what strategies we can take to promote cybersecurity innovation and best practices.

Thank you, Mr. Chairman. I yield back.

[The statement of Hon. Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

MAY 28, 2025

Good afternoon, everyone.

Between the talent on this campus and the numerous companies started in Silicon Valley, I am honored to join our Nation's innovators today. You not only build the solutions we need to stay ahead of threats, but also have the creativity to identify the problems that Congress can't even imagine.

Thank you for your interest in our hearing and your partnership.

Our enemies aggressively target U.S. critical infrastructure through novel techniques and persistent campaigns. Volt and Salt Typhoon, 2 China-backed threat actors, demonstrate that America's foreign adversaries are intent on finding weaknesses in our cybersecurity wherever they can. It is therefore crucial that America's cybersecurity capabilities remain ahead of the foreign actors who aim to harm us, and that our technology is secure.

Staying ahead of our adversaries requires a whole-of-society approach—one that unlocks the full potential of our innovative capacity to address and prevent vulnerabilities in our IT and OT. Silicon Valley will be crucial to this effort because many of our cybersecurity leaders are here. Silicon Valley companies are often the front-line defense against cyber attacks, and they will help develop solutions to bolster our homeland defense.

Ensuring we build and use the right cybersecurity solutions requires a strong partnership between the public and private sectors.

The foundation of this collaboration is information sharing—a key focus for my subcommittee this Congress. Information sharing between the public and private sectors is beneficial not only for staying ahead of threat actors, but also for driving innovation to where it is needed most.

By sharing information about emerging threats and empowering CISA to manage cross-sectoral relationships, information sharing will help develop the tools we need to understand how threat actors operate in cyber space.

Innovation plays a critical role in keeping up with new tactics, techniques, and procedures of threat actors as our adversaries attempt to compromise U.S. networks by any means necessary.

My subcommittee recently held a hearing on an important authority—the Cybersecurity Information Sharing Act of 2015, otherwise known as CISA 2015. Information sharing between the public and private sectors heavily relies upon this vital authority, so it is imperative that Congress reauthorizes CISA 2015 before it expires later this year.

I am also pleased that we are talking about regulatory harmonization during today's hearing. This is a topic which my subcommittee has explored extensively, especially in the context of CIRCIA—the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Industry's feedback is critical to obtain an effective, final rule that meets Congressional intent, which is why I look forward to hearing your perspectives on the current regulatory landscape.

Our expert panelists have led the charge in protecting the United States from threats to our cybersecurity.

I look forward to hearing your insights into what strategies we can take to promote cybersecurity innovation and best practices.

Chairman GREEN. Thank you, Mr. Garbarino.

It is always difficult to have an official hearing in your own district. This happens to be Mr. Swalwell's district, and I am certain, as I would be if we were having this hearing in my district, he is pulled in a thousand different ways. So we will have him make his opening comments after our witnesses if he gets here by then.

I am pleased to have a distinguished panel of witnesses with us today. Their incredible experience in this evolving landscape of cyber, whether in government or private sector, will help shed a lot of light today on the challenges and solutions that we need in cyber space.

I will ask the witnesses to stand and raise their right hand.

[Witnesses sworn.]

Chairman GREEN. Let the record reflect that the witnesses have answered in the affirmative.

Thank you. Please be seated.

I would now like to formally introduce our witnesses. The Honorable H.R. McMaster is a senior fellow at the Hoover Institution at Stanford University. He is a proud graduate of West Point and served as a commissioned officer in the United States Army for 34 years, retiring in the rank of lieutenant general in 2018.

He won the Silver Star as a company commander in one of history's very most famous tank battles in Desert Storm. He served as the Nation's 25th National Security Advisor from 2017 to 2018.

Ms. Wendi Whitmore is the chief security intelligence officer at Palo Alto Networks. She is a globally-recognized cybersecurity leader with 2 decades of experience in building incident response and threat intelligence teams.

She began her career as a special agent conducting computer crimes investigation with the United States Air Force, Office of Special Investigations.

Ms. Jeanette Manfra, did I pronounce that correctly?

Ms. MANFRA. Yes.

Chairman GREEN. OK. She is the global director for the security and compliance at Google Cloud. Prior to joining Google, she served as the assistant director for cybersecurity at CISA.

Ms. Manfra spent more than a decade serving in various roles of the Department of Homeland Security and the White House, focused on establishing the Nation's first civilian Cyber Defense Agency.

Jeanette is a proud veteran in the U.S. Army and I believe an Army aviator.

Mr. Jack Cable is the CEO and co-founder of Corridor, an organization that helps companies performing AI-powered security refractors at scale. He previously served as a senior technical advisor at CISA where he helped lead the work on Secure by Design and open-source software security.

I thank our witnesses for being here today, and I now recognize General McMaster for 5 minutes to summarize his opening comments.

STATEMENT OF HERBERT RAYMOND "H.R." McMASTER, SENIOR FELLOW, HOOVER INSTITUTION, STANFORD UNIVERSITY

General MCMASTER. Chairman Green, Congressman Garbarino, Congressman Swalwell, and Members of the subcommittee, it is a privilege to testify before this committee at a critical moment for our Nation and the free world.

I hope that my statement for the record is useful to you in the important work that this committee is undertaking to understand U.S. cybersecurity posture and develop solutions to improve critical infrastructure, resilience, foster technological innovation, and harmonize regulations.

It is a particular privilege to be on this panel alongside 3 private-sector innovators and great Americans who have done vital work to help maintain our competitive advantage in cyber space.

This hearing is timely because, as has already been mentioned, in recent years responses to adversaries' state attacks have been slow and inadequate. Strengthening deterrence will require the rapid imposition of costs on cyber attackers that go far beyond those that those attackers anticipate prior to acting against us.

We must also improve the resilience of our systems through a combination of defensive and, as you mentioned, Mr. Chairman, offensive capabilities, as well as the capacity for rapid recovery.

We must maintain competitive advantage in artificial intelligence, quantum computing, and other technologies relevant to cybersecurity and the associated protection of critical infrastructure.

Chairman Green, as you already mentioned, particularly important are going to be removing barriers to implementation of cyber space solutions and AI models. I think that is a particularly important aspect of getting from information to action, as you mentioned.

We must improve dramatically the security of our critical technologies and research enterprises from the threat of relentless state-based espionage.

Accomplishing these tasks will require close cooperation between the public and private sectors and academia and with international partners, as well as investments in research and I would say especially human capital.

Maintaining our advantage in human capital should include attracting the best talent to our universities and granting visas to graduates who can help grow our Nation's talent base in science and engineering.

Thank you. It is a real privilege to be with you.

[The prepared statement of General McMaster follows:]

PREPARED STATEMENT OF LTG H.R. MCMASTER (U.S. ARMY, RETIRED)

28 MAY 2025, 2 O'CLOCK PM PDT

This committee's work to understand U.S. cybersecurity posture and develop solutions to improve critical infrastructure resilience, foster technological innovation, and harmonize regulations is vitally important. And this panel's focus on how the United States can raise the cost of cyber attacks and strengthen deterrence is timely because, in recent years, responses to adversary state attacks have been slow and inadequate.

In 2017 during President Trump's first term, his national security team prioritized the competitive domains of cyber space and space as part of his integrated national security strategy. Emphasis was on protecting critical infrastructure

as well as data, sensitive technology, and intellectual property. We were particularly concerned about the security of what we labeled the National Security Innovation Base (NSIB), defined as the network of knowledge, capabilities, and people, including academia, National Laboratories, and the private sector, that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life. The NSIB develops technologies (such as those associated with fifth-generation communications (5G), artificial intelligence, quantum computing, and biogenetics) that are vital to maintaining America's advantages in defense and in the global economy.

Since 2017, despite efforts to improve the security of the NSIB and protect critical infrastructure, data, and technology, the threat in cyber space has grown due to AI advancements and the increased connectivity of physical objects to cyber space. To reduce the threat from malicious cyber actors, the United States and its allies must enhance both offensive and defensive cyber capabilities. We must also improve system and infrastructure resilience through cooperation across Government, businesses, and academia. And, consistent with the premise of this hearing, it is vital to integrate all elements of national power and efforts of likeminded partners to impose high costs on nation-states and non-state actors that attack or threaten our Nation through cyber espionage or attacks.

AI technologies are making cyber attacks easier as more of the physical world becomes connected to cyber space and the malicious actors who operate within it. AI technologies can defeat encryption and allow systems to perform tasks usually reserved for humans such as hacking through firewalls. Combined with communications networks such as 5G, supercomputers (and eventually quantum computing), and the "internet of things" (i.e., the internet of computing devices embedded in everyday objects), an AI-enabled cyber attack could affect everything from power grids to public transportation to financial transactions to global logistics to driverless cars to home appliances. As the Volt Typhoon discovery revealed, People's Republic of China (PRC) cyber actors are already on IT networks and possess the capability to conduct disruptive or destructive cyber attacks against U.S. critical infrastructure.

Deterrence by denial requires a combination of offensive and defensive capabilities, resilient systems, and a high degree of cooperation across Government, businesses, and academia. Unfortunately, such cooperation is a challenge in our decentralized, democratic systems. During the first year of the Trump 45 administration, our NSC staff worked to remove bureaucratic impediments to timely identification and response to cyber threats. I was frustrated with the slow progress, but new authorities combined with General Paul Nakasone's superb leadership of NSA and U.S. Cyber Command improved our responsiveness. But there is much more that we can do to foster cooperation across the public and private sectors.

Deterrence by denial and effective response to cyber attacks also requires actions against hostile cyber actors that extend beyond the cyber domain. Those include sanctions and financial actions, but they are often inadequate. It is sometimes difficult to hold something of value to an adversary or an enemy at risk. Elusive terrorist and criminal organizations hide their leadership and other important assets. And as hostile regimes like Iran and North Korea come under increased international and internal pressure, their leaders may conclude that they have little to lose. A physical military response may be appropriate and necessary against actors that prove difficult to deter. And it is important to convince difficult-to-deter adversaries that they cannot accomplish their objectives through a cyber attack because our defenses are strong and we can recover rapidly.

The threat to infrastructure critical to U.S. security extends far beyond the shores of North America. The CCP's ambition is to control physical as well as digital infrastructure to achieve dominance of global logistics and supply chains. The vanguard of this twenty-first-century conquest is China's state-owned and state-sponsored enterprises, including telecommunications, port, and shipping companies. Democratic, free-market economies continue to furnish the CCP with "rope" as China has set about acquiring a global maritime infrastructure that complements its control of communications infrastructure. China has targeted E.U. countries and other U.S. allies such as Israel for control of ports. And many of these ports under Chinese control, such as Antwerp, Trieste, Marseille, and Haifa, are located near clusters of scientific and industrial research facilities. By 2020, according to China's Ministry of Transport, 52 ports in 34 countries were managed or constructed by Chinese companies, and that number was growing.[1] That is why it will be important to share this committee's work with allies and partners and urge the Trump administration to

[1] Yaakov Lappin, "Chinese Company Set to Manage Haifa's Port, Testing U.S.-Israeli Alliance," South Florida Sun Sentinel, January 29, 2019, *https://www.sun-sentinel.com/florida-jewish-journal/fl-jj-chinese-company-set-manage-haifa-port-20190206-story.html.*

coordinate a multinational response to these threats as well as common standards for how their governments interact with the private sector and with one another when it comes to how data is managed and how it is collected, processed, stored, and shared.

Strong defense and rapid recovery require common understanding and increased cooperation across the public and private sectors. Organizations like the Cyber Policy Center here at Stanford play a vital role in fostering common understanding. The Defense Innovation Unit and the Cybersecurity and Infrastructure Security Agency (CISA) are examples of how to structure such collaboration. Additionally, technology companies must be aware of the geopolitical implications of their innovations, avoiding complicity in aiding authoritarian regimes. Collaboration among scientists and between scientists and policy makers is vital for innovation. Here at the Hoover Institution we have been fostering common understanding and cooperation to counter threats through seminars under the Tech Track II Dialogue and sustained assessments of critical technologies under the Stanford Emerging Technology Review. The need for collaboration on crucial challenges to national security is growing because technology-based innovation is shifting away from governments and toward the private sector. To take full advantage of opportunities and protect against dangers in space and cyber space requires an understanding of how technologies interact with one another and humanity. That is the premise of the Stanford Institute for Human-Centered Artificial Intelligence.

Private-sector companies that specialize in cybersecurity and countering cyber espionage hold promise to bridge the divide between the tech sector and Government. It is important for engineers at tech firms to know how adversaries use cyber space and emerging technologies and to be aware that their firms are competing against not only other companies, but also hostile nations. The ability of companies, universities, and research organizations to contract capabilities in cyber defense, counterintelligence, and data recovery is growing. Private-sector efforts that overlap with those of governments could lead to better civil-military coordination and cyber defense burden sharing. The line between Government and private-sector intelligence and security is blurring. Government would benefit from contracting cutting-edge commercial capabilities. And it is likely that some private-sector companies will conclude that they need to be active on adversary networks to detect and preempt attacks on their systems, data, or intellectual property. Because companies that go offensive in cyber space risk incurring foreign government penalties, assuming liability for harm inflicted on innocent third parties, and sparking an escalation to armed conflict, public- and private-sector coordination is essential for integrating offense and defense in cyber space.

A counterintuitive but key defensive action is, in addition to having a plan to recover rapidly from attack, to design cyber networks and systems for graceful degradation under the assumption that they will be attacked relentlessly. Exquisite systems based on the latest technology may be prone to catastrophic failure. Resiliency must be a critical design parameter not only for weapon systems, but also for communications, energy, transportation, and financial infrastructure. Resiliency requires keeping suspect hardware and software off networks and continuously identifying and, when appropriate, preempting enemy attacks. We must recognize that allowing hardware from companies such as China's Huawei or ZTE into our communications networks is tantamount to opening Troy's gates to the mythical Trojan horse. Purchasing other hardware from Chinese companies is also irresponsible as we have discovered with cranes and solar panels. Vigilance must be habitual and integrated into company and governmental operational culture. And vigilance must be comprehensive across a company's OT, IT, hardware, and supply chains. Third-party risk is particularly difficult to manage.

Every company that develops sensitive technology or holds critical data should treat that technology and data like gold and strive to make their company or research organization "Fort Knox." Prior to the end of the Cold War, the U.S. model of technological development was relatively closed, meaning that the Government funded and controlled access to major initiatives such as nuclear weapons, jet fighters, and precision-guided munitions. These programs were protected by security classifications, patents, and copyrights. When the Government decided to declassify technologies such as microchips, touch screens, and voice-activated systems, private-sector engineers and entrepreneurs combined and refined those technologies to kick-start new industries such as the smartphone. In the twenty-first century, technological innovation truly opened up. Innovations increasingly derive from diffuse publicly-financed research. Meanwhile, China has implemented its top-down military-civilian fusion strategy to steal technology and direct investments with the intention of surpassing the United States in strategic emerging industries (SEIs) and military capabilities.

For too long much of academia, the private sector, and the Government were oblivious to how adversaries can steal and apply technologies developed in the United States to threaten security and undermine human rights. Congress should prohibit U.S. capital from accelerating the CCP's efforts to surpass the United States in a range of critical emerging technologies, such as quantum computing and AI-related technologies, important to achieving military superiority. Seven hundred Chinese companies, the majority of which are state-owned or -controlled, are traded in the U.S. debt and equity markets. U.S. citizens still fund companies that are building the next generation of the PLA's military aircraft, ships, submarines, unmanned systems, and airborne weapons. Until recently U.S. venture capital investment in Chinese AI companies exceeded investment in U.S. companies. Many U.S. and allied executives and financiers go beyond the quotation attributed to Vladimir Lenin that "The capitalists will sell us the rope with which to hang them." They are financing CCP's acquisition of the rope. The easiest first step in strengthening deterrence might be to stop underwriting our demise.

Chairman GREEN. Thank you, General McMaster.

I now recognize Ms. Whitmore for 5 minutes to summarize her opening statement.

STATEMENT OF WENDI WHITMORE, CHIEF SECURITY INTELLIGENCE OFFICER, PALO ALTO NETWORKS

Ms. WHITMORE. Chairman Green, Congressman Garbarino, and Congressman Swalwell, thank you for the opportunity to testify today on innovation in cybersecurity, including how our adversaries are intensifying their attacks and, more importantly, how we can innovate to turbocharge our defenses.

My name is Wendi Whitmore, and I am the chief security intelligence officer at Palo Alto Networks.

Palo Alto Networks is an American cybersecurity company founded in 2005 and has since become a global cybersecurity leader. We support 97 of the Fortune 100's, the U.S. Federal Government, critical infrastructure operators, and a wide range of State and local partners.

The breadth and depth of the organizations that we help protect gives us a unique vantage point into the cyber threat landscape, and what we see is very concerning.

As recent campaigns like Salt and Volt Typhoon have reinforced, our cyber adversaries, China, Russia, Iran, North Korea, and others, are more active and aggressive than ever. They are leveraging AI to increase the speed and scale of their attacks, to enhance tactics like phishing, exfiltrate data faster, and execute complex multistage attacks that are increasingly disruptive to the American public.

Consider this. Every single day Palo Alto Networks blocks up to 31 billion cyber attacks. Up to 9 million of those daily attacks represent novel attack methods never previously seen.

To stay a step ahead, relentless innovation must be central to our cyber defenses. Innovation with AI at its core has the potential to disrupt the legacy status quo of chasing each new threat with an isolated, disjointed solution.

Instead we can leverage AI to analyze security data in real time and then automate our responses. This evolved approach can simultaneously, No. 1, deliver transformative cybersecurity outcomes; No 2, drive much-needed cost rationalization; and, No. 3, eliminate inefficient manual processes.

Palo Alto Networks supports this committee's desire to pivot away from a stale, point-in-time, compliance-first mindset for cyber

resilience and radically rethink how AI and automation can modernize our cyber defenses.

The potential impact here is not hypothetical. We have seen our customers dramatically improve their cyber defenses. With AI-powered security operation centers, their average response times to cyber attacks have dropped from 2 or 3 days to under 2 hours. This is a transformative shift.

Palo Alto Networks is proud to be an integrated national security partner with the Federal Government. My written testimony includes a series of recommendations policy makers should consider at this pivotal moment for our Nation's cyber defense. Let me take a moment to focus on a few of those.

First, focus on measurable cybersecurity outcomes. Ensure cybersecurity investments improve agencies' basic cyber vital signs by reducing the mean time to detect and the mean time to respond to security incidents.

Second, forcefully respond to Salt Typhoon by implementing zero trust. This evolved security approach does not implicitly grant access, and it can limit the impact of these attacks.

Third, fully embrace AI to support cyber defense. Network defenders are drowning in data as they manually triage alerts. AI has the power to modernize security operation centers and allow analysts to be more proactive in their threat hunting.

Fourth, promote secure AI by design. To safely harness the incredible power of AI, enterprises must have the frameworks and capabilities to discover, assess, and protect against threats to AI infrastructure.

At the end of the day people, processes, and technology must work in concert. Palo Alto Networks applauds Chairman Green's reintroduction of the Cyber PIVOTT Act to help foster a steady pipeline of trained cyber professionals and begin addressing our Nation's cybersecurity work force gap.

We continue to see productive collaboration take place across a range of cybersecurity-focused convening bodies, including CICA's Joint Cyber Defense Collaborative. We support Representative Swalwell's efforts to put wind in the sails of JCDC's mission.

Critical to sustaining an enduring partnership is the free exchange of cyber threat intelligence across the public and private sector. To that end, we support swift reauthorization of the Cyber Information Sharing Act of 2015 and appreciate the thoughtful hearing Representative Garbarino convened on this issue earlier this month.

Palo Alto Networks takes a partnership with law enforcement and lawmakers and this committee seriously.

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

[The prepared statement of Ms. Whitmore follows:]

PREPARED STATEMENT OF WENDI WHITMORE

MAY 28, 2025

Chairman Green, Ranking Member Thompson, and distinguished Members of the committee: thank you for the opportunity to participate in today's hearing. I appreciate this committee's commitment to understanding cybersecurity threats facing our Nation and how to best equip the defenders on the digital front lines. My name

is Wendi Whitmore, and I am the chief security intelligence officer for Palo Alto Networks.

For those not familiar with Palo Alto Networks, we are an American cybersecurity company founded in 2005 that has since become the global cybersecurity leader—protecting over 70,000 enterprises across more than 150 countries. We support 97 of the Fortune 100, critical infrastructure operators of all shapes and sizes, the U.S. Federal Government, universities and other educational institutions, and a wide range of State and local partners.

My testimony outlines the increasing sophistication of cyber adversaries and sheer volume of cyber attacks our customers defend against daily. In fact, every day we block up to 31 billion cyber attacks. Of this total—up to 9 million of those daily attacks—represent novel attack methods never previously seen.

To stay a step ahead, we must be relentless in our commitment to cyber defense innovation. To that end, Palo Alto Networks is proud to have invested $1.8 billion in R&D just last year. We are confident that this innovation—with AI at its core—can disrupt the status quo of the cybersecurity industry and simultaneously: (1) Deliver transformative cybersecurity outcomes, (2) drive much-needed cost rationalization for network defenders, and (3) eliminate inefficient, manual processes. This innovative spirit will be critical to combatting not just the threats of today, but also the emerging risks—like encryption-breaking quantum computing—of tomorrow.

Palo Alto Networks supports this committee's desire to pivot away from a stale, point-in-time, compliance-first mindset for cyber resilience—and instead radically rethink how AI and automation can turbocharge cyber defense. While policy makers appropriately cultivate a robust and on-going debate about the right combination of carrots and sticks to incentivize desired outcomes, one thing is clear: "business as usual" in the cybersecurity ecosystem is failing to translate cybersecurity investments into cybersecurity outcomes. We look forward to working with all interested parties to chart out a more resilient path forward.

THE EVOLVING CYBER THREAT LANDSCAPE

At Palo Alto Networks, we have a unique vantage point into the cyber threat landscape. What we are seeing should concern us all. Our cyber adversaries—China, Russia, Iran, North Korea, and beyond—certainly aren't sitting on their hands.

In May 2023, we contributed to the first U.S. Government advisory on the China-attributed Volt Typhoon campaign against a range of critical infrastructure entities. Since then, another China-linked campaign, called Salt Typhoon, rightfully garnered substantial attention from cyber practitioners and policy makers for its successful targeting of communications infrastructure.

These campaigns, and others, highlight a sobering reality—adversaries can also be innovative. They are actively leveraging emerging technologies, like AI, to amplify the scale and speed of their attacks and to find new vectors to compromise systems. Attackers are leveraging AI for deepfake-enabled social engineering, enhancing ransomware negotiations, and identifying sensitive credentials. The emergence of Agentic AI, autonomous systems capable of making decisions and adapting tactics without human intervention, poses a significant escalation of this threat. In the future, Agentic AI will be able to independently execute multi-step operations, leading to faster, more adaptive, and difficult-to-contain cyber attacks.

Meanwhile, the pace of AI adoption across companies and industries vastly increases the total size of the digital attack surface that can be exploited by adversaries, even further complicating the cyber defense picture.

Palo Alto Networks distills these cyber threat landscape trends in our annual incident response report, informed by our work assisting victims of over 500 major cyber attacks. These incidents involved large organizations grappling with extortion, network intrusions, data theft, advanced persistent threats, and more. The targets of these attacks spanned all major industry verticals across 38 countries. Our analysis of these engagements highlights several important trends:

- *Increasing Business Disruption*.—Threat actors are augmenting traditional ransomware and extortion with attacks designed to intentionally disrupt victim operations. In 2024, 86 percent of incidents that we responded to involved business disruption—spanning operational downtime, reputational damage, or both. Attackers are using this disruption to force victims into negotiating and paying a ransom.
- *Cyber Attacks Are Moving Faster Than Ever*.—Attackers exfiltrated data in under 5 hours in 25 percent of incidents in 2024, which is 3 times faster than in 2021. What's even more alarming is that in 1 in 5 cases, data theft occurred in under 1 hour.

- *AI Is Accelerating the Attack Life Cycle*.—AI has the potential to significantly reduce the cost of creating customized malware, creating conditions for a significant surge in malware variants that will be more difficult to defend against with traditional cyber capabilities. In a controlled experiment, our researchers found that AI-assisted attacks could reduce the time to exfiltration to just 25 minutes, a 100x increase in speed.
- *Phishing Makes A Comeback*.—After vulnerabilities took the top spot in 2023, phishing resurged as the most common entry point for cyber attacks, responsible for 23 percent of all initial access. Fueled by generative AI, phishing campaigns are now more sophisticated, convincing, and scalable. Inclusive of phishing, 44 percent of the attacks we investigated in 2024 involved a web browser—heightening the importance of browser security.
- *Complexity Is Killing Security Effectiveness*.—In 75 percent of incidents, logs existed that should have indicated potentially malicious activity. But, data silos prevented detection before it was too late.
- *Multipronged Attacks Are the New Norm*.—In 70 percent of incidents, attackers exploited 3 or more attack surfaces, forcing security teams to defend endpoints, networks, cloud environments, and the human factor in tandem.
- *Elevated Insider Threat Risk*.—Organizations face an elevated risk of insider threats, as nation-states like North Korea target organizations to steal information and extort victims for funding which they then use to support national initiatives. Insider threat cases tied to North Korea tripled in 2024.
- *Increasing Cloud Attacks*.—Nearly 29 percent of cyber incidents involved cloud environments, with 21 percent causing operational damage to cloud environments or assets as threat actors embedded within misconfigured environments to scan vast networks for valuable data. In one campaign that compromised a cloud environment, attackers scanned more than 230 million unique targets for sensitive information.

MEETING THE MOMENT: LEVERAGING AI FOR CYBER DEFENSE

Despite the evolving threat landscape, we remain confident that we are well-equipped to combat the cyber incursions of today and tomorrow. AI is, and will continue to be, a game changer, not only for the bad guys, but also for the cyber defenders who ward off the crooks, criminals, and nation-states that threaten our digital way of life. Our product suite, which spans network security, cloud security, endpoint security, and Security Operations Center (SOC) automation, leverages AI to stay a step ahead of attackers.

Palo Alto Networks first introduced machine learning (ML) capabilities as part of our malware protection offering 10 years ago. We now deploy over 30 products that leverage AI, with many more in development. Our Precision AI combines the best of ML, deep learning, and generative AI to drive real-time and automated security.

Looking forward, these benefits will continue to increase as cyber professionals incorporate more Agentic AI capabilities into their defense portfolio. Here, AI-powered cyber capabilities will help automate remedial, often human-driven operations, to allow the platform to automate certain response actions and decrease the time it takes for an organization to respond to an incident.

Empowering Cyber Professionals

For too long, our community's most precious cyber resources—people—have been inundated with security alerts that require manual triage, forcing them to play an inefficient game of "whack-a-mole," while vulnerabilities remain exposed and critical alerts are missed. Making matters more difficult, this legacy approach often requires defenders to stitch together security data from across dozens of disparate cybersecurity products at the same time. Organizations find themselves drowning in their own data, struggling to operationalize it. Industry research shows that over 90 percent of SOCs are still dependent on manual processes, a sure-fire way to give adversaries the upper hand and increase analyst burn-out.

This inefficient, manual posture results in suboptimal performance against metrics like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to incoming incidents. Metrics like these serve as basic cyber vital signs for an enterprise's security posture. They provide quantifiable data points for network defenders about how quickly they discover potential security incidents and how quickly they contain those incidents. Historically, organizations have struggled to execute against these metrics. In fact, a report by Unit 42 found that security teams average nearly 6 days to resolve an alert in cloud breach incident response cases.

AI-Driven Security Operations Centers

AI-driven SOCs can flip this paradigm and give defenders the upper hand. This technology acts as a force multiplier for cybersecurity professionals to substantially reduce detection and response times. The results from deploying this technology on our own company networks are significant:

- On average, we ingest 90 billion events daily.
- Using AI-driven data analysis, this is distilled down to 26 thousand raw alerts.
- This is further triaged to just 1 incident that requires manual SOC investigation.

We then deployed this AI-powered SOC to our customers where we are seeing similarly transformative outcomes:

- Reduction of MTTR from 2–3 days to under 2 hours, with ~60 percent of customers under 10 minutes.
- Five-fold increase in incident close-out rate.
- Four-fold increase in the amount of security data ingested and analyzed each day.

These dramatic improvements are critical to stopping threat actors before they can encrypt systems or steal sensitive information—which is now frequently happening in mere hours. None of this would be possible without the power of AI.

COMMITMENT TO CYBERSECURITY INNOVATION—PROTECTING AGAINST EMERGING RISKS

Securing AI by Design

AI is taking enterprise IT by storm, and it is here to stay. On the commercial side, 42 percent of enterprises are already leveraging AI tools. This is expected to grow to 96 percent within the next 12 months, with over 12,000 AI apps projected to be in use by 2030. AI use is also surging in the U.S. Federal Government, where 41 Government agencies reported a total of 2,133 AI use cases for the Consolidated 2024 Federal AI Use Case Inventory, up from just 710 use cases reported for 2023. The typical large enterprise will use hundreds of AI apps internally, leverage thousands of AI models, and produce many petabytes of training and vector embedding data annually.

This expanded AI attack surface brings evolved data security and network security challenges. Research indicates that 50 percent of employees currently use AI apps without permission in their enterprise, 80 percent of public models can be "jailbroken" (bypassing restrictions installed by model creators), and there are already hundreds of malicious models available in the wild.

In sum, AI app proliferation is changing how enterprises operate. This change demands an evolved security approach. We like to think of this approach as Secure AI by Design. This approach requires the ability to:

1. *Discover*.—Gain a clear understanding of AI assets being developed across the enterprise.
2. *Assess*.—Continuously assess security, safety, and compliance risks of AI apps, agents, models and datasets, across the supply chain and runtime.
3. *Protect*.—Detect and prevent risks detected in the supply chain and runtime.

These principles are aligned with, and based on, the security concepts already included in the NIST AI Risk Management Framework (RMF).

Fully harnessing the enormous potential of AI requires deploying it securely. Furthering our commitment to lead this important AI security conversation, we recently announced our intention to acquire ProtectAI, an early innovator in this space.

Ensuring Quantum Readiness Today

AI is also accelerating quantum R&D, bringing the era of encryption-breaking quantum computers closer than previously anticipated. This forthcoming moment of quantum reckoning is likely to render existing public key encryption, the foundational underpinning of data security for the last several decades, obsolete and insecure. Accordingly, we must move aggressively to harden our systems for the inevitable post-quantum cryptographic reality.

While the U.S. Government has commendably established a 2035 time line for Federal agencies to transition to quantum-safe cryptography, the reality of "harvest now, decrypt later" attacks demands a far more aggressive posture. Adversaries are actively collecting our sensitive encrypted data today, fully intending to decrypt it within the coming years. Waiting until 2035 to achieve comprehensive quantum readiness will leave a significant window of vulnerability, jeopardizing Classified information and the personal data of American citizens.

To effectively counter this risk, the United States must adopt a more proactive and accelerated approach to quantum readiness. We urge Congress to prioritize quantum readiness in all Federal IT modernization initiatives, ensuring that new

systems are built and procured with post-quantum cryptographic compatibility from the outset. Further, we must incentivize the adoption of quantum-safe technologies across the critical infrastructure sectors that underpin our national security and public safety. Central to this imperative will be leveraging solutions that empower organizations to continuously inventory their cryptographic vulnerabilities, visualize and prioritize risks, and implement quantum-safe remediations through automated workflows.

Bottom line: we believe 2035 may be too late. Quantum readiness requires decisive action now.

POLICY RECOMMENDATIONS TO DRIVE FEDERAL CYBER RESILIENCE

Palo Alto Networks is proud to be an integrated national security partner with the Federal Government and stands ready to help. To that end, we developed a set of recommendations for policy makers to consider at this pivotal moment for our Nation's cyber defense:

1. *Focus on measurable cybersecurity outcomes*.—Are cybersecurity investments actually making networks safer? Two of the most telling indicators of cyber resilience are MTTD and MTTR. The President should be able to walk into the White House Situation Room and see the real-time cyber vital signs, like real-time MTTD and MTTR metrics, for all agencies.
2. *Forcefully respond to Salt Typhoon by promoting Zero Trust*.—This is an evolved security approach with a layered, continuous reverification posture that does not implicitly grant access. It requires end-to-end visibility and an enhanced focus on mobile core and management plane security.
3. *Embrace the multicloud reality—but don't forget security*.—Cloud is becoming the dominant attack surface—in a Unit 42 report, over 80 percent of vulnerabilities observed by our team were cloud-based. The increasing trend of multicloud adoption further challenges the legacy-shared responsibility model for security. In response, we must aggressively promote cross-cutting cloud security tools that provide both visibility and operational control.
4. *Leverage AI to empower cyber defense*.—Cyber professionals are drowning in alerts that they must manually triage. They need AI-powered tools to flip this paradigm and stay ahead of adversaries, like China. There is a particular opportunity to leverage AI to modernize SOCs, and Palo Alto Networks applauds the recently-signed EO on Removing Barriers to American Leadership in Artificial Intelligence as an important validation of AI's enormous national security potential.
5. *Promote Secure AI by Design*.—To fully harness the incredible power of AI, enterprises (including Federal agencies) need to enforce access controls, harden deployment environment configurations, and ensure data integrity across AI supply chains.
6. *Promote Defense Industrial Base (DIB) resilience*.—The DIB is a natural extension of our national security apparatus, and it is under constant attack by adversaries. In response, we should further expand the scope and scale of DIB cybersecurity services offered by the NSA Cybersecurity Collaboration Center.
7. *Modernize Federal procurement*.—Current procurement cycles do not operate at the speed of technological innovation, giving adversaries the upper hand. For example, there is far too much reliance on legacy VPN tools (increasingly targeted by adversaries) instead of modern Zero Trust solutions.
8. *Make meaningful progress on cybersecurity regulatory harmonization*.—The Federal Government can lead by example by consolidating and streamlining Federal Government software compliance certifications. For example, there should be logical reciprocity between FedRAMP High and DoD IL–5 certifications.
9. *Operationalize the Federal Acquisition Security Council (FASC)*.—Established during the first Trump administration, this can be a critical tool to ensure the technology in our Federal enterprise is trustworthy with appropriate supply chain integrity.
10. *Leverage cyber shared services to increase efficiency and reduce waste*.—Shared service offerings for Federal agencies can provision cybersecurity capabilities at scale—improving cybersecurity outcomes while being prudent stewards of taxpayer dollars.

PEOPLE AND PARTNERSHIPS

To stay ahead of cyber threats, we need people, processes, and technology working in concert. To that end, Palo Alto Networks applauds Chairman Green on the reintroduction of the Cyber PIVOTT Act. The bill's recognition of the importance of

collaboration between the Government, community colleges, and industry, and the power of hands-on, skills-based exercises, will help build a pipeline of skilled professionals capable of protecting our digital way of life.

We are also working to broaden access to cybersecurity education. The Palo Alto Networks Cybersecurity Academy offers free and accessible curricula, aligned to the NIST National Initiative for Cybersecurity Education (NICE) Framework, to academic institutions from middle school through college. Hands-on experiences with cyber and AI benefit the entire ecosystem as they help to upskill our own workforce as well as that of our customers.

Palo Alto Networks also offers several accelerated onboarding programs to help broaden our workforce, including the Unit 42 Academy. As full-time members of our incident response and cyber risk management teams, early career professionals with both university and military backgrounds spend 15 months developing skills through specialized, instructor-led courses, on-the-job training, and mentorship.

Partnership is in our DNA at Palo Alto Networks, and our collective defense depends upon deepening collaboration between industry and Government. We are active members of the Information Technology Sector Coordinating Council (IT–SCC), and participate in several projects—including zero trust network architecture, quantum security, and 5G security—at the National Cybersecurity Center of Excellence (NCCoE).

We continue to see productive collaboration across a range of cybersecurity-focused convening bodies, including CISA's Joint Cyber Defense Collaborative (JCDC). With that in mind, we support Rep. Swalwell's efforts to further put wind in the sails of the JCDC, which has been a great partner for those in industry.

Maintaining the ability to share cyber threat intelligence across the public and private sectors remains vital, and we fully support reauthorizing the Cyber Information Sharing Act of 2015. We appreciate the thoughtful hearing Rep. Garbarino convened on this issue earlier this month.

We take our partnership with lawmakers—and this committee—seriously. Please consider Palo Alto Networks a standing resource as you continue to consider cybersecurity and AI issues. Thank you for the opportunity to testify. I look forward to your questions.

Chairman GREEN. Thank you, Ms. Whitmore.

I now recognize Ms. Manfra for 5 minutes to summarize her opening statement.

STATEMENT OF JEANETTE MANFRA, GLOBAL DIRECTOR FOR SECURITY AND COMPLIANCE, GOOGLE CLOUD

Ms. MANFRA. Thank you, Chairman Green and Garbarino, Ranking Member Swalwell. Thank you for the opportunity to appear before you today and for your focus on this important issue.

As was said, my name is Jeanette Manfra, and I am the head of global risk and compliance for Google Cloud. We appreciate you holding this important hearing, and we do look forward to sharing Google's perspective on opportunities for regulatory harmonization and compliance modernization to better enable our entire ecosystem to protect itself against the rising threats.

Technology advances as do the threats, and cybersecurity defenders must adapt to it all if we want their approaches to stay current. In an interconnected world facing growing cyber attacks, it is critical to ensure that technology systems are resilient and keep people safe.

For nearly 20 years, Google has pioneered both Secure by Design and Zero Trust Architectures, which means that we embed security into every approach of our software development life cycle, including looking at physical security throughout our entire stack.

At Google Cloud, we believe in something we call shared fate, which moves beyond shared responsibility and indicates less of a transactional relationship in the security responsibilities, but it shows that we are investing in our own security, in our infrastruc-

ture, in our platforms, in our software, but we are also investing in ensuring that our customers can be secure and compliant and modernize their own systems.

Regulating cybersecurity at the national scale though is complex, poses unique challenges, and carries high stakes. Regulatory and compliance regimes impact the resilience of critical infrastructure, economic development, the pace of technological innovation, military deployments and capabilities, and the daily lives of American citizens.

As a result, cybersecurity regulation should be carefully balanced, promoting strong cybersecurity baseline standards while allowing flexibility to account for evolving technology and the ever-changing threat landscape.

At Google, we recommend a regulatory approach that is agile and focuses on aligning baseline requirements across sectors. The approach must also allow for additional sector-specific requirements that are complementary to and not duplicative of or in conflict with those standard baselines.

This approach would increase adoption of security principles across the Federal Government, critical infrastructure, and the wider private sector.

Regulatory agility will help reduce compliance burdens, enhance coordination, build public trust, and allow for a more resilient approach as the threats change, new economic sectors emerge, and agency responsibilities change and shift over time.

I believe regulations must prioritize tangible outcomes over mere checklists. Google's commitment to openness, interoperability, transparency, responsibility, a Secure-by-Design approach, intelligent security systems, and collaborative efforts can only be fully realized within such an adaptable regulatory environment.

We urge Congress to modernize cybersecurity regulations and create a stable baseline that existing sectors can adhere to and future sectors can adopt as a reliable guide for improving security and resilience.

To achieve regulatory harmonization, I will offer just a few central recommendations. First, leveraging well-established standards and processes for any contemplated security baseline approach.

In our view, initiatives like the Federal Risk and Authorization Management Program, or FedRAMP, is well-established and we are very supportive of GSA's efforts to modernize this, including through initiatives like FedRAMP 20X that looks at increased automation.

We further encourage leveraging capabilities like the Open Security Controls Assessment Language, or OSCAL, for more streamlined authorizations.

Second, any harmonized standards should implement a risk-based approach, ensuring compliance options are aligned to specific risk levels or categories to maximize flexibility and efficiency commensurate with the level of risk associated with the particular technology, application, or usage case.

Finally, complement harmonization through a clear approach to reciprocity for different certification regimes.

As the committee considers mechanisms to achieve regulatory harmonization, we also urge the Members to continue to foster

public-private dialog on the topic and to look at a global harmonized approach to ensure enterprise and service providers can focus on security outcomes as a top priority.

We remain committed to the security of a digital ecosystem and we are pleased to continue to engage with you all in future cybersecurity regulations.

[The prepared statement of Ms. Manfra follows:]

PREPARED STATEMENT OF JEANETTE MANFRA

MAY 28, 2025

Chairmen Green and Garbarino, Ranking Members Thompson and Swalwell, and distinguished Members of the committee; thank you for the opportunity to appear before you today. My name is Jeanette Manfra, and I am the senior director for global risk and compliance for Google Cloud. We appreciate the House Committee on Homeland Security holding this important hearing, and we look forward to sharing Google's perspective on opportunities for regulatory harmonization and compliance modernization to enable the entire ecosystem to better protect itself against rising threats.

Technology advances, threats evolve, the cybersecurity landscape changes, and cybersecurity defenders must adapt to it all if they want their approaches to stay current. In an interconnected world facing growing cyber attacks, it is critical to ensure that technology systems are resilient to keep people safe. For more than 20 years, Google has pioneered a Secure-by-Design approach, meaning we embed security into every phase of the software development life cycle—not just at the beginning or the end.

Google Cloud offers a suite of world-class security solutions, including identity and access management, data security, network security, incident response services, threat intelligence, and much more. We are proud to have been a pioneer of zero trust architectures, and we are committed to partnering with customers to ensure they can deploy securely in the cloud while meeting their compliance obligations through every step of their cloud migration journey. At Google Cloud, we believe in a Shared Fate model that goes beyond traditional shared responsibility. We work closely with our customers to achieve optimal security and risk outcomes, and we continuously invest in robust security capabilities and transparency protocols to maintain the most trusted platform.

As we continue to pursue excellence in security for ourselves and our customers, we also believe there is an opportunity to modernize our approach to compliance.

IMPORTANCE OF REGULATORY HARMONIZATION AND RECOMMENDATIONS

Regulating cybersecurity at the national scale is complex, poses unique challenges, and carries high stakes. Regulatory and compliance regimes impact the resilience of critical infrastructure, economic development, the pace of technological innovation, military deployments and capabilities, and the daily lives of American citizens. As a result, cybersecurity regulation should be carefully balanced: promoting strong cybersecurity baseline standards while allowing flexibility to account for evolving technology and the ever-changing threat landscape.

Google recommends a regulatory approach that is agile and focuses on aligning baseline requirements across sectors. The approach must also allow for additional sector-specific requirements that are complementary to and not duplicative of or in conflict with those standard baselines. This approach would increase adoption of security principles across the Federal Government, critical infrastructure, and the private sector. Regulatory agility will help reduce compliance burdens, enhance coordination, build public trust, and allow for a more resilient approach as threats change, new economic sectors emerge, and agency responsibilities change and shift over time.

Regulations must prioritize tangible outcomes over mere checklist compliance. Google's commitment to openness, interoperability, transparency, responsibility, a secure-by-design approach, intelligent security systems, and collaborative efforts can only be fully realized within such an adaptable regulatory environment. We urge Congress to modernize cybersecurity regulations and create a stable baseline that existing sectors can adhere to and future sectors can adopt as a reliable guide for improving security and resilience.

To achieve regulatory harmonization, Google offers a few central recommendations. First, leverage well-established standards and processes for any contemplated

security baseline approach. In our view, initiatives like the Federal Risk and Authorization Management Program (FedRAMP) are already established with support from the public and private sector. We welcome GSA's work to modernize the FedRAMP program, including through increased automation, and we further encourage leveraging Open Security Controls Assessment Language (OSCAL) for more streamlined authorizations. Second, any harmonized standards should implement a risk-based approach—ensuring compliance options are aligned to specific risk levels or categories to maximize flexibility and efficiency commensurate with the level of risk associated with a particular technology, application, or use case. And finally, complement harmonization through a clear approach to reciprocity for different certification regimes (such as FedRAMP levels, DoD SRG Impact Levels, and other existing or future programs).

As the committee considers mechanisms to achieve regulatory harmonization, we also urge Members to continue to foster public-private dialog on the topic. We encourage the committee to consider a global harmonized approach to ensure enterprises and service providers can focus on security outcomes as a top priority. Google remains committed to the security of the digital ecosystem and would be pleased to consult on future cybersecurity regulations.

Thank you for convening this important hearing. We look forward to continuing to further raise awareness about cybersecurity threats and defenses, and the work we are doing at Google Cloud to keep networks protected.

Chairman GREEN. Thank you, Ms. Manfra.

I now recognize Mr. Cable for 5 minutes to summarize his opening statement.

STATEMENT OF JACK CABLE, CEO AND CO-FOUNDER, CORRIDOR

Mr. CABLE. Chairman Green, Chairman Garbarino, and Ranking Member Swalwell, thank you for the opportunity to testify here today.

My name is Jack Cable. I am the CEO and co-founder of Corridor, a company using AI to make Secure by Design a reality. Our platform understands the security model of the code base, refactors on safe code, and adds guardrails around AI coding assistance.

This hearing is a deeply personal topic for me. We are here at Stanford, my alma mater where I studied computer science. Throughout my career as a self-taught ethical hacker working in the private sector, academia, and Government, I prided myself on finding innovative solutions to the hardest problems in cybersecurity.

Most recently I helped lead CISA's work on Secure by Design and open-source security and created the Secure-by-Design pledge.

As this committee has highlighted, state-sponsored hackers from the People's Republic of China are burrowed within our critical infrastructure. Should China invade Taiwan, they stand to conduct destructive cyber attacks on our power grids, water systems, telecom providers, and more.

But these attacks are not inevitable. Most cyber attacks exploit preventable vulnerabilities in softer products or insecure default configurations. This could be as simple as a default password that sits unchanged.

Rather than placing the burden on end-users like small businesses or school systems, software manufacturers must build Secure-by-Design products, thus raising costs on our adversaries. This is our best hope to defend against PRC's cyber threats and the time to act is now.

Today I will focus on 3 areas for urgent action: securely adopting AI, Secure by Design, and strengthening security research.

First, AI. A revolution is under way in software development. It is now possible to build a website with just a single prompt. The vast majority of developers now use AI coding assistance, enabling them to ship software faster than ever before. This will unlock tremendous innovation and advancements in productivity.

At the same time, these tools can introduce vulnerabilities. Studies show that even top AI models write vulnerable code 30 to 40 percent of the time. It is only a matter of time until AI coding assistance introduces a severe vulnerability in critical software that is exploited.

At Corridor, we are helping companies embrace AI securely. Our platform adds guardrails to AI assistance preventing them from introducing vulnerabilities in the first place.

As AI adoption accelerates, these kinds of protections must become the norm, and I encourage Congress to foster R&D to enable rapid software development without compromising on security.

Second, Secure by Design. At CISA, we were often asked if Secure by Design would stifle innovation. As someone building my own company, I can say with confidence that the opposite is true. The same design decisions that make systems secure by default also produce higher-quality code that costs less to maintain.

Though over 300 companies who voluntarily committed to CISA's pledge is another sign that security and innovation can go hand in hand, buyers can also shift market incentives. Last month JPMorganChase published a letter urging their vendors to prioritize security, noting that poor security practices are actively enabling cyber attacks.

At CISA, we call this Secure by Demand. The U.S. Government should lead by reforming procurement. Today's check-the-box, compliance-oriented processes focus more on enterprise security than the actual security of products. It is like checking that a factory has locked its doors without testing the quality of the products that it produces.

CISA's secure software development's self-attestation form is a good start. Congress and the administration should build on this by incorporating more outcomes-based product security measures in procurement, drawing from CISA's pledge and the product security bad practices list.

Third, security research. The PRC has enacted laws requiring security researchers to report vulnerabilities to the Chinese government before disclosing to vendors.

I recently published a piece with Jen Easterly advocating for Congress to respond by strengthening the open-entrance parent security research ecosystem in the United States, recognizing that security researchers like myself can play a vital role in discovering and reporting vulnerabilities before our adversaries can.

While we have made progress, laws like the Computer Fraud and Abuse Act, or CFAA, continue to chill security research. Congress should reform the CFAA and associated laws to exempt good-faith security research, building on DOJ's work to discourage illegal action against ethical hackers.

Additionally, the Common Vulnerabilities and Exposures, or CVE, Program is an essential resource for tracking vulnerabilities

and their root causes. This program must continue, and all companies should issue complete, accurate, and timely CVE records.

Congress should codify under CISA the CVE program's essential mission as a national record of security flaws.

In closing I would be remiss not to recognize the exodus of technical talent that has occurred at CISA over the last several months. I have personally seen how CISA has lost its very best.

In the face of increasing threats, we cannot undermine the capacity of America's cyber defense agency and its ability to attract and retain the best technical talent. This only makes us less secure as a Nation.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Cable follows:]

PREPARED STATEMENT OF JACK CABLE

MAY 28, 2025

Chairman Green, Ranking Member Thompson, Chairman Garbarino, and Ranking Member Swalwell, it is my honor to testify here today.

My name is Jack Cable. I am the CEO and co-founder of Corridor, a company using AI to help make secure by design software a reality. Our platform can understand the security model of a codebase, refactor unsafe patterns, and add guardrails around AI coding assistants.

This is a deeply personal topic for me. We're here at Stanford, my alma mater, where I studied computer science. Throughout my career, I've prided myself on finding innovative solutions to the hardest problems in cybersecurity. As a self-taught ethical hacker, I've worked in the private sector, academia, and government to advance the state of software security. Most recently, I helped lead CISA's Secure by Design and open-source software security initiatives, including creating the Secure-by-Design pledge, where hundreds of companies have committed to demonstrating their progress in securing their software.

I've seen first-hand how insecure software can jeopardize our public safety, particularly as both nation-state actors and cyber criminals seek to compromise our Nation's critical infrastructure. And I've seen how technological advancements like AI can both help improve our collective state of security and magnify existing vulnerabilities.

As this committee has highlighted, state-sponsored hackers from the People's Republic of China are currently burrowed within our critical infrastructure. Should China invade Taiwan, they stand to conduct destructive cyber attacks on our power grids, water systems, telecom providers, and more.

But these attacks are not inevitable, nor unpreventable. The vast majority of cyber attacks take advantage of either a preventable software vulnerability or an insecure default configuration.[1] This could be as simple as a temporary default password intended to be changed right away that sits unchanged. Rather than placing the burden on end-users to take care of these problems, software manufacturers can build their products to be secure by design and thus raise costs on our adversaries. Secure-by-design software is our best hope to defend against PRC cyber threats. The time to act is now.

THE PROMISES AND PERILS OF AI

There is a revolution happening in software development right now. It's now possible to build a website with just a one-sentence prompt. The overwhelming majority of developers are now using AI coding assistants,[2] enabling them to ship software faster than ever before.

AI coding models can introduce the same vulnerabilities that we've known about for decades. Studies have found that even the best models write vulnerable code

[1] *https://hbr.org/2024/04/preventing-ransomware-attacks-at-scale.*
[2] *https://github.blog/news-insights/research/survey-ai-wave-grows/.*

about 30–40 percent of the time.[3] [4] It's only a matter of time until AI coding assistants introduce a severe vulnerability in critical software that is exploited.

At Corridor, we're using AI to secure software without slowing down development. With our technology, we can add guardrails to AI assistants, preventing them from introducing vulnerable code in the first place. Companies adopting AI coding assistants must take a proactive stance and enact guardrails now.

We also need to make sure that current and future software developers understand the basics of security. Alarmingly, none of the top 20 degree programs in computer science require a course in security to graduate. We wouldn't let civil engineers graduate without understanding how to build safe bridges. So why do we allow software engineers to get a degree without knowing how to build secure systems?

SECURE BY DEMAND

At CISA, we were often asked whether Secure by Design would stifle innovation. As someone who's building my own company today, I can say that there doesn't have to be a trade-off between security and innovation. The security of a software system is a property of the overall quality of the software. The same design decisions that make our systems more resilient and secure by default also lead to higher-quality code that costs less to maintain. The fact that over 300 companies voluntarily committed last year to CISA's Secure-by-Design Pledge is another sign that security and innovation can go hand-in-hand.

By working together, we can accelerate the pace of adoption of Secure-by-Design practices—and this takes everyone, including software manufacturers and their customers. Last month, the chief information security officer of JP Morgan Chase published a letter saying that third-party software suppliers are enabling cyber attacks, and urging them to prioritize security.[5]

At CISA, we called this "Secure by Demand". All software customers can help to raise the bar for the product security of their vendors.

The U.S. Government should play a key role by doing away with check-the-box, compliance-oriented procurement processes and starting to measure actual product security practices. Today, far too many requirements focus on the enterprise security practices of the company building the software, rather than the actual security of the product itself. This is akin to testing that a factory has locked its doors, but not evaluating the products that the factory is producing.

CISA's Secure Software Development Self-Attestation form is a good starting point. I encourage Congress and the administration to expand on this to include more outcomes-based product security measures, such as from CISA's pledge and the Product Security Bad Practices list, to further incentivize software manufacturers to build their products with security from the start.

CVES AND VULNERABILITY DISCLOSURE

I recently published a piece with former CISA Director Jen Easterly advocating for Congress to strengthen the security research ecosystem in the United States.[6] Security researchers like myself play a crucial role in discovering and reporting vulnerabilities before our adversaries can.

The PRC has enacted laws to require security researchers to report vulnerabilities to the Chinese government before disclosing to vendors. We must counteract this with an open and transparent security research ecosystem in the United States.

While we've made progress in recent years, anti-hacking laws like the Computer Fraud and Abuse Act (CFAA) still have a chilling effect on good-faith security research. Congress should reform the CFAA—and associated laws such as Section 1201 of the Digital Millennium Copyright Act (DMCA)—to exempt good-faith security research. The Department of Justice has worked over the last decade to demonstrate an understanding in the value of good-faith security research and to discourage legal action against ethical hackers. Nonetheless, as with other laws that protect unintended targets of legal action, the security community should not and cannot rely solely on prosecutorial discretion to protect good-faith security research from legal retaliation.

Additionally, the Common Vulnerabilities and Exposures (CVE) program is an essential resource for tracking vulnerabilities and their root causes. We must ensure

---

[3] *https://baxbench.com/*.
[4] *https://dl.acm.org/doi/full/10.1145/3610721*.
[5] *https://www.jpmorgan.com/technology/technology-blog/open-letter-to-our-suppliers*.
[6] *https://www.lawfaremedia.org/article/advancing-secure-by-design-through-security-research*.

that this critical program continues and that all companies issue complete, accurate, and timely CVE records for their vulnerabilities.

Congress should codify, under CISA, the CVE program's essential mission as a national record of security flaws, and normalize vulnerability disclosure by eliminating barriers to security research.

CONCLUSION

In conclusion, we must act now to secure the threats of today, and those that will come tomorrow. By addressing the risks posed by AI, raising the bar through Federal procurement, and fostering a healthy security research ecosystem, we can fundamentally secure software and raise costs on our adversaries.

Finally, I would be remiss not to recognize the exodus of technical talent that has occurred at CISA over the last several months. I have personally seen how CISA has lost its very best. In the face of increasing threats, we can't undermine the capacity of America's Cyber Defense Agency and its ability to attract and retain the best technical talent. This only makes us less secure as a Nation.

Thank you. I look forward to your questions.

Chairman GREEN. Thank you for your testimony, all of you, and I now recognize my friend and the host here of this district or the Congressman from this district, Mr. Swalwell, for 5 minutes.

Ranking Member, you are recognized.

Mr. SWALWELL. Yes. Thank you, Chairman, for coming to the Bay Area.

My district is just right across the bridge. Sam Liccardo now represents this district, but the Chairman has a deep interest in this area geographically but also this area is an issue.

So thank you, Chairman. We have had a good visit, and I also want to thank my friend Mr. Garbarino. We are the quietest subcommittee in the Homeland Security Committee room. There is a lot of news that is made in that room, but when Mr. Garbarino and I have our hearings, it is usually a snoozefest for anyone who wants drama because we are trying to get things done, and the Chairman, Chairman Green, has enabled us to do that.

Thank you to our witnesses for participating. General, thank you to you for your service to our country, and thank you to Stanford for hosting this.

My interest in this area, I represent Lawrence Livermore National Laboratory and Sandia National Laboratory, and they work in this space and in the private sector.

We have many, many not only start-ups but giants in this space, and so I am in the solutions business, and I know the 2 gentlemen up here are as well, and my priority is this Congress, and I want to hear from these witnesses as I juggle this hearing and a meeting 2 floors upstairs.

My priority is to really leverage the private sector, make sure that the Federal Government is as additive as possible, and as you pointed out, Ms. Whitmore, to reform the JCDC if we can to make it, you know, more responsive, have more structure and scaffolding as far as criteria, and make sure it is a two-way information sharing network, not just the private sector sharing with the Federal Government.

So in the spirit of getting to these questions and hearing from the witnesses, I will submit my remarks to the record, Mr. Chair, and I will yield back.

[The statement of Hon. Swalwell follows:]

STATEMENT OF HONORABLE ERIC SWALWELL

MAY 28, 2025

I want to thank Chairman Green, Ranking Member Thompson, and Chairman Garbarino for coming to the Bay Area for this field hearing. I also want to thank our panel of witnesses for joining us today.

Their collective public and private-sector experience will help us better understand the cyber threats facing our country and how we can best leverage innovation to improve our security. There is no better place than here in Silicon Valley to have this conversation about the innovative technologies that will shape our cybersecurity future.

I have benefited tremendously during my time in Congress from the expertise of technology leaders here in the Bay Area, and I am glad to see a recognition that the Homeland Security Committee more broadly can gain valuable insights from the Silicon Valley tech community. I hope that today's hearing will help further build the connections to facilitate conversations between Silicon Valley and Congress going forward.

As we have seen, technological progress offers tremendous opportunities but also creates new security risks. Recent advances in AI technology have enabled more sophisticated phishing attacks, and deepfake technologies have helped North Korean hackers gain access to computer networks by pretending to be remote job applicants. As our adversaries seek to utilize these new technologies, they continue to invest in advanced technologies like quantum computing that will render current encryption standards ineffective.

In order to compete, we must continue to invest in innovation and move quickly to integrate the best technologies available into our cyber defenses. I hope to learn more today from our witnesses on how technology is shaping the current threat landscape and how threats are likely to evolve in the coming years so that we can ensure the Federal Government is staying ahead of our adversaries.

I also look forward to hearing more about how we can better leverage new technologies for our own cybersecurity and how we can better support the cybersecurity technology ecosystem. Having today's hearing at Stanford University is the perfect venue to highlight the importance of sustained public-private partnerships in technological innovation. The emergence of Silicon Valley as the leading technology center in the world was no accident.

It was the presence of one of the world's leading research universities that helped bring together global experts in one place for research and for training new innovators, spurring private-sector growth throughout the region. It was also a diverse immigrant community with some of the leading technology and business minds from around that world that found a welcoming place to start and develop new technology companies.

And it was vital Federal investments in research and development that helped spur the creation of the internet and many of the innovations that have transformed our world. Without that symbiotic relationship between Government, academia, and the private sector, many of the leading technology companies would not be headquartered here in Silicon Valley or even in the United States.

I worry that the current administration's efforts to cut funding for universities and for research and development and to cut immigration and student visas will undermine our Nation's ability to innovate going forward. As China continues to ramp up its research and development, we cannot afford to pull back our public investment in technological development and universities. Doing so would harm our economic competitiveness and our national security.

Today's hearing will help the committee learn about how that public-private collaboration has fueled innovation and how we must build on that collaboration going forward. We also must ensure that both the public and private sectors are well-positioned to implement new technologies rapidly.

CISA plays an incredibly important role in facilitating public-private collaboration, including through the JCDC, and supporting the development to cybersecurity best practices, like Secure by Design, that can help lift the cybersecurity baseline across the technology ecosystem. Continued support for CISA's efforts will be necessary to support the utilization of innovative technologies going forward, and I hope our witnesses will help us understand how CISA can best fulfill its role in supporting innovation.

Chairman GREEN. Thanks.

I think the only bipartisan legislation or I should say all of the bipartisan legislation I have done in this Congress and last Congress was with you, Eric. So thank you.

I want to thank our witnesses for their insightful testimony, and the Members are going to be asking a lot of questions, and I will start with those questions myself.

Honestly, we have got plenty of time. So I am going to take as long as I want to. OK?

[Laughter.]

Mr. GARBARINO. You will not mind if I interrupt.

Chairman GREEN. The witnesses generated a lot more. I am taking furious notes.

One of the things that shocks me is how uninformed the American people seem to be on just how pervasive the attacks against this Nation are in cyber space, the Salt and Volt Typhoon being an example.

I think I was speaking at Crowd Strike or someplace. It was in the District of Columbia when I said this, when I first coined this phrase, but having that intrusion into our cell phone systems or telecoms, imagine if Russia placed a satchel charge next to a cell tower and had a detonator in their hand.

We would be livid, but essentially that is exactly what China has done to our telecommunications systems, right, Mr. Cable? You brought it up very well in your testimony.

Yet there is no clamor about this on the television. There are no, you know, alerts or reels. They literally have a kill switch in the system right now and nobody is making a big deal out of it.

Why do you guys think that is the case?

I will throw that out to any one of you who wants to answer.

General MCMASTER. I will just say, first of all, I think because we have not really taken this to the American people to explain the gravity of it. I think, to really ask the question, "OK. Well, why? You know, why is China on our systems?"

Mr. Cable, I think, alluded to it. It is because I think they are preparing for war.

Chairman GREEN. Yes.

General MCMASTER. The Chinese Communist Party is preparing for war in a number of ways, right? We see it with their massive build-up of the military forces, about a 44-fold increase in their defense spending since the year 2000.

We see it in the development of weapons systems just to keep us at bay, but also, I think what we can do is connect what we have seen with Volt Typhoon to a broader range of threats, including the massive build-up of their nuclear forces, about a 400 percent increase.

I know it may seem extreme to say this, but I believe that China is developing a first-strike nuclear capability against us because why else would you want to cripple all of your critical infrastructure, including communications infrastructure?

If you look at the pattern of their intelligence collection, for example, the balloon intelligence collection was really aimed at communications intelligence that can only be picked up at that altitude, and that was communications intelligence associated with our strategic forces.

So I think the American people have not really had this explained in context, and maybe we need something like, you know, the old movie, "The Day After," you know, that shows what it would look like, something like what was done with "The Social Dilemma" movie, you know, to kind-of bring it home to people.

But that is something, Chairman Green, I think we can take on here at the Hoover Institution, is to sort-of package an understanding of this threat and communicate that as effectively as we can.

Chairman GREEN. Yes, I think that is something that is part of the reason why we are here, not only to get the information from you guys, but to be on TV so the American people can hear from you guys.

Deterrence, I have always thought of deterrence as the product, not the sum of capability and will. You can have all of the capability in the world and zero will and you get zero deterrence. Zero times infinity is still zero.

So if you guys could make some comments about what you think we need to do better in terms of capability and then in terms of will, I know that is a broad topic, but I am thinking about, really how do we establish deterrence in the cyber space?

Maybe, Ms. Whitmore, you can take a shot at that.

Ms. WHITMORE. Absolutely, and, Chairman Green, I think further to your earlier question as well as the General's commentary here, my viewpoint on this has been from 20 years of responding on the ground to some of the most major breaches that have occurred in the last few decades.

You know, many of those when I started my career in the military were highly-Classified investigations that no one talked about and certainly could not be talked about in open dialog. So that certainly contributed to the lack of awareness from the public.

I think it is a great movement in the right direction that we now can have such an open dialog, but the reality is in addition to the lack of awareness, I think one of the things that we unfortunately do today is punish the victims.

So what I mean by that is when, you know, for example, a bank robbery, we oftentimes do not publish that on the news and blame the bank for, you know, having an armed robber come in at gunpoint and a teller provide them some funds that are in their tray.

But when the media gets hold of cases of cyber crime and these massive intrusions, we do often do that, and then we add regulation in that requires them to provide information in this most dynamic time period, the first 48 to 72 hours, very similar to traditional crimes. That is also the time that it is most dynamic in a computer intrusion.

So you have a victim who is now potentially trying to negotiate or have communications with an attacker. They are working with law enforcement. They are working with outside legal counsel, and they still do not have all the technical details of an investigation that are needed to fully answer these questions and understand is this a national security issue; is this potentially a cyber criminal that could potentially be related to a terrorist or criminal organization.

So I think that, as we are talking through solutions here, there are a lot of technical recommendations which certainly Palo Alto Networks would provide about, hey, greater capabilities in the hands of the victims so that they can get answers quickly.

But there is also the component of it of what can we do from a Government lens of making sure that we are providing as much support as possible to the victims so that we do not expect a small-to-medium business to effectively, to use your terminology, go up against some of the greatest military capability that our foreign adversaries have to offer.

Chairman GREEN. Yes. I am going to go from the hundred thousand foot down to like, Mr. Cable, you talked about Secure by Design, and this is more at the tactical level.

Your company, if I understand it correctly, is out there trying to help other developers develop their products secure from the beginning, the whole point of the reversing of the economic model.

One of the questions I ask is I am a physician. I ran a health care company. If I developed a medical device that looked really great, we put it in 200,000 people and then it turns out to be faulty and it harms those individuals. I am done. I have lost everything, and my company is going to pay a big price, probably go out of business.

Why is it that a software company that can put an app out there that has a vulnerability in it is no big deal?

How is that fair?

Can you explain something about that?

Mr. CABLE. Thank you, Chairman, for the question.

To your point, this is not fair, and to build on what Ms. Whitmore was saying, this is not a fair fight. If we look to the small businesses, the hospitals, the school systems who have been facing these attacks, whether they are ransomware attacks, whether they are state-sponsored actors, this is not a fair fight.

We cannot rely on these under-resourced organizations to be able to defend against sophisticated cyber criminals and nation-state threats.

Really we need to, to your point, take a step back and look at the security of the technology that is underpinning our critical infrastructure.

The fact is that today in many ways we are leaving our doors open to our Nation's adversaries. They are able to compromise our critical infrastructure through relatively simple, preventable vulnerabilities in software products, and the software companies are not incentivized or held responsible for these vulnerabilities.

At CISA, we worked to advocate for software companies to both voluntarily increase their security through the Secure-by-Design pledge which both Google and Palo Alto Networks, for instance, are signatories of.

We worked to make sure that companies were really pushing to be cutting-edge and taking actions like reducing entire classes of vulnerabilities from their products.

I am generally optimistic that we can root out these vulnerabilities from our software products, but this is going to take time, and it is really going to take shifting incentives.

So there is, I think, good room to be had for discussions around what I mentioned with Secure by Demand, getting private companies, getting the Government to start to demand better security practices from software suppliers.

But I do also think we need to consider a software liability regime by which manufacturers of software products are held accountable for preventable vulnerabilities in those products and, of course, that we give sufficient safe harbor protections to ensure that there is a bar that software manufacturers can reach.

Chairman GREEN. Well, I appreciate your answer on that because it is a tough one. I, you know, talk to some of the biggest companies in the world that make both hardware, software, operating systems, all of it, the whole gamut, and they do not want product liability, you know.

Being in the military, I am going to ask one more question. Then I will turn it over to Mr. Garbarino.

Being a military guy, I think courses of action, and 3 military folks and a guy who worked in the Government, so you probably have heard that term before, courses of action. What are the courses of action?

So you look at a ransomware attack, for example. You know, if we are going to come up with solutions to how do we stop this stuff, we have to have courses of action.

On the extreme, one I have heard which on the surface sounds sort of anti-Republican, anti-private sector, anti, but on some level makes some sense to me, is just outlaw the payment of a ransomware. A couple people get hit at the beginning. There are some costs to those entities because their systems are—maybe we have a fund that can help cover that, but at some point the bag guys are not going to get paid.

They know they are not going to get paid, and that would be ultimate deterrence for ransomware. What are your thoughts?

Ms. Manfra.

Ms. MANFRA. I do not think it would be effective to outlaw payment.

Chairman GREEN. OK.

Ms. MANFRA. But I wanted to go to your point on deterrence.

Chairman GREEN. Let me make sure I have this. Not to outlaw ransomware.

Ms. MANFRA. Payments. You can outlaw ransomware.

Chairman GREEN. I am saying outlaw payments of ransomware.

Ms. MANFRA. Yes.

Chairman GREEN. You can outlaw drugs and they are everywhere, right? It is ubiquitous. But I mean to outlaw the payments.

Ms. MANFRA. The payments, yes. We should look at and discuss it some more for sure, but I think it is just such a complicated space right now and you run into scenarios where you potentially have life and safety issues without that payment. So there are lots of things you would want to take into consideration.

Chairman GREEN. Sure.

Ms. MANFRA. It is worth considering, continuing that conversation though.

On a higher level, when you talk about deterrence, and it is something that I have thought about a lot and we have thought

about as a company, too, is I think that there are a couple of different elements of thinking about deterrence, and oftentimes they get conflated when we are talking about cybersecurity.

You know, when you are thinking about and people say deterrence by denial, right? You know, make our defense excellent so they cannot get through, and that is a real thing that we need to continue to invest in, but then you also talked about capability and will for not just that deterrence by denial, denying their ability to get into the system, denying an ability to take the actions that they are seeking to.

But I would say there is also thinking about, and much more clear-eyed, the risks that our country faces. So we need that stable baseline. We need to raise the level of security. All of our attackers are still taking advantage of very easily-known vulnerabilities that should be fixed.

I agree that both, you know, software vendors and others in the community, there needs to be some accountability mechanisms in place to ensure that we are delivering secure and safe software and then, of course, the accountability in place to make sure that people are using it correctly.

So if there is one effort that needs to be focused on, how do we stop just the continued poor performance in known security issues.

But then there is another effort which the JCDC played some part in this and I think CISA can continue to lean in here, is there are unique national risks that impact certain sectors more than others and require a different set of capabilities and perhaps a smaller set of actors that have capabilities in the private sector and the Government coming together to identify what is the threat, how are we going to counter that threat, who has the capabilities to do that in a collective way, and that requires a new type of public-private partnership that is just as important as raising that baseline and making sure every small business has what they need.

But we also need to be focused very much on reducing the consequences of the next time we find China or some other actor in these critical systems, and we need to be opening up that dialog and that operational collaboration between the companies and the entities in the Government to do much more work in reducing those national risks for those foreign actors who would hold our country at risk.

Chairman GREEN. Yes. I am going to make a quick comment and then I am going to let Mr. Garbarino have a couple of minutes.

You said something there that was very interesting to me. The next time we find China in the system, so to speak, and this is something that my staff will tell you they have been hearing me say this for years. It is unfair for the Federal Government to expect the private sector to defend itself against a nation-state. We, particularly my side of the aisle, have pushed very hard about a sovereign border, having a sovereign border that needs to be protected, and that the Government has a responsibility to protect.

You know, if China were physically driving tanks across the Southern Border, that is exactly what the Federal Government would do, would be to defend against that.

But I would submit that there is a cyber border that is just as sovereign, and we cannot expect companies to defend themselves, and I think it is going to take a paradigm shift because for decades we have taken this free-market approach that private sector takes care of itself. Government takes care of itself.

Again, I think that is self-defeating because the networks are so connected now wherever a person enters, they can pretty much move laterally anywhere in the networks. The Government shares cloud space with companies and Amazon.

So I just want to say that I could not agree with you more, and I want to reiterate this to whomever is paying attention. The Federal Government has a responsibility, and we need to step up and partner and do it more. Do it more and better.

Mr. Garbarino, you are recognized.

Mr. GARBARINO. Thank you, Mr. Chairman.

I wanted to jump in a couple of times because I was writing down questions, too, based on some of their answers. If you hear something and they say, "Please jump in," like I said, we have time, and I am sure Mr. Swalwell will come down. He has always got great questions, too, when we have committee.

But your first thing you brought up about why do people not care more, and I think it is because we have not really felt pain in the country. There is no cyber attack. People who have gotten individual attacks have felt it, you know. Companies who have gotten ransomware, they have felt it.

But I went to Estonia. You approved a trip for us to go, a cyber trip, to Estonia 2 years ago, and they had the major cyber attacks, I think, back in 2007, and they all take cybersecurity very seriously there.

Now, we have not had that yet but for a few, and again, you know, there were gas lines on the East Coast for a couple of days. I mean we have not felt real pain. So I think that is a problem.

I really appreciate what we are doing here and what the witnesses are doing here because we are trying to be preemptive or proactive here and trying to fix something before we actually feel real pain.

So I do appreciate you all being here, and, Mr. Cable, I want to go back to something you said talking about holding designers accountable. How would you?

Because I love the idea of Secure by Design. I love the work that CISA did, and I love the work that all the companies that took that pledge do. I think that is great. I think there should be, you know, a reliance when somebody buys something that there is at least some security, especially when you are talking about whether it is a phone or a computer program or a computer, whatever. There should be some reliance that there is some security there and they can depend on that without having to pay extra.

But then you also have to go back and you have to weigh that against user error. I mean, somebody clicks on something. That is a click. You are only as strong as your weakest link.

So, you know, you can hold a company accountable for its design up to a point, I believe, but at some point the balance tips and goes to, well, yes, but people automatically think, OK, this is secure. I

can just do whatever I want. I get that. I mean, there still has to be some reliance on the individual.

So how do we weigh that?

Who holds the companies accountable if you hold the companies accountable, and how do you hold them accountable? Is it financial? What is it?

I would love to hear from everybody on this actually.

Mr. CABLE. Thank you, Congressman, for the question.

I agree that there is a balance to be struck, and this is an area that we focused on through the Secure-by-Design work at CISA.

One aspect of Secure by Design we call Secure by Default, this idea that configuration out of the box of a software product should be a secure one, just like when you buy a car and it comes with seatbelts, air bags by default. You do not have to pay extra for those.

We should also expect that security features are really built into software products. In my opening statement, I mentioned the example of a default password where there are still products on the market that come out with a default password, and the expectation is that the end-user of that product goes and changes the password.

I am sure we have all been there. We know that that does not always happen, and the question that we ask at CISA is why does that responsibility have to be on the end-user? Why does the manufacturer of the product, as many do, not ship the product with, say, a random password so that it is more secure by default?

So that is really what we are talking about when we mean Secure by Default, and I agree that there is an extent where users can go and change configurations and at some point it does go out of the manufacturer's control.

But often what we are talking about are not complicated scenarios. It is where a user takes the product out of the box, deploys it, and it is susceptible to some vulnerability that is enabled by default.

So really when it comes to shifting incentives, to what I was saying earlier, I think it is essential to consider how we can help take this burden off of end-users, off of small businesses, hospitals, and others who really do not have the capacity, nor should they, to defend against these attacks and see how software manufacturers can assume more of this responsibility.

That was the focus with the Secure-by-Design pledge where companies, now over 300 companies who committed to that, commit to taking action in areas like reducing default passwords across their products, increasing the use of multi-factor authentication such as by enabling that by default, which we know can prevent cyber attacks, and reducing common classes of vulnerabilities.

So I think there are lots of areas and potential really for software manufacturers to innovate on the basis of security, to compete based on that, and I encourage this committee to think about how it can help to shape some of those market——

Mr. GARBARINO. Well, what is the incentive?

I mean, is it a Government pushing saying, "OK. These have met the Secure-by-Design standard"?

So what are we saying? Like, OK, in order for a financial institution to take part in the FDIC protection, you have to have this.

I mean, what is the incentive? Is it carrot? Is it stick?

I mean, what are we doing to make sure that these things fall? Please, everybody jump in.

Mr. CABLE. Yes. One thing that I would note is I think today when we look at the cybersecurity regulations and requirements, those are almost always placed on the end-users of technology products, its requirements on financial companies or hospitals or others who really, and I think to the point of this discussion, are not the most resourced or the most capable of applying those.

Really where I think we need to go is to look at, OK, how can we help shift some of those requirements off of those least responsible, off of those who really are not fit to go up against a nation-state, and help to rebalance the responsibilities so that they are placed on the software manufacturers who are most capable and the best positioned to take care of that.

So I think that could be done through the Federal purchasing power, through private-sector purchasing power, through software liability regime really with end goal of not moving to an unreasonable standard but at least having some baseline by which we can make sure the software products we rely on throughout our critical infrastructure are more Secure by Design.

Mr. GARBARINO. Ms. Manfra.

Ms. MANFRA. Sure, and if I could, I agree, and if I could add that the clarity of the standard and the requirement for transparency, too, right?

Security is very hard for users, customers, and so I do think there are incentives on the software industry to make security easier actually. But we need to increase the demand for that, and the Federal Government has an opportunity through their purchasing power to do that through standards, whether that is through certification regimes or others.

But then also mandating transparency, you know, at Google we have been pushing things like what we call salsa, but where you have artifacts that say this is how the code was tested so you can see the provenance of the code and you can have a higher level of assurance of the integrity of that.

Making sure that, you know, every time you buy a microwave, right, you know that it has gone through testing and you understand and you may not know every single detail of what that testing was, but you know that it has received a certification and that it has been allowed to be sold to you.

So there is more work that could be done there for sure in establishing what those baseline standards are and the Federal Government has a real opportunity to drive that, what those standards are, driving more certifications around it.

But then I would say there needs to be much more transparency and it needs to be just easier for a procurement official, for that end-user to be able to understand what they are buying and that it is clear how it is meeting their security requirements.

So the Government also has an obligation to set I would say clearer security standards that are more consistent across the Government. Those are all opportunities, I think, that all companies would welcome that participation with the Government on.

Mr. GARBARINO. Any other additions?

General MCMASTER. Just a quick comment because this goes to Chairman Green's comment earlier about how so much of our attack surfaces in the dotcom and in the public sector rather than in the Government sector.

I think there should be a convergence of standards between dotgov and dotcom. All companies should strive for that.

I think there are also some best practices that should be followed that everybody should share with one another as we create this community of really companies or anybody who touches critical infrastructure with their products.

That is kind-of a holistic approach to security involving we are talking a lot, you know, about IT, but it is OT, it is hardware, it is supply chain, and then it will not be until we are all together on these standards that you can really reduce what is really critical, which is that third-party risk, you know, which we have seen really go through the roof in recent years in terms of software and supply chains that can have a devastating effect if they are compromised.

I think that what is really key and I think what we are talking about, and I would love to hear the full panel's thoughts about this, there is a tension between setting a standard and holding companies accountable for it and not treating the company like a victim because you want them to report.

Really what you want is the Government and that company to be working together when something bad happens, and overall, I mean, companies, I think, have to kind-of adopt the attitude of try to envision like what we do in the military. What is the worst thing that could happen to you, right? Then take action to prevent that, right?

What you would do the day after a massive attack is what you should do right now, you know, and so I think how to think about these complex challenges and then the melding together of dotgov and dotcom standards and this holistic approach to security, which I would say, and I mention in the statement for the record, includes, you know, not just threats in cyber space but insider threats as well because you know the CCP. When you close the front door, it comes through the window. If you put bars on the window, they are putting a ladder to the second floor. You close that down and they are tunneling into your basement, and they will do it in the physical world through espionage as well as in cyber space.

Ms. WHITMORE. I certainly agree with so much of the commentary that, you know, my fellow witnesses have shared, and Palo Alto Networks is a strong supporter and signatory of Secure by Design as well.

I think something that has been resonating here is just how challenging it is to maintain visibility into the attack surface as it continues to expand. So we are looking at supply chain vulnerabilities, right? We are really figuring out how do we manage every single software provider that anyone in the organization may have procured software through.

That is very challenging. I think we need to continue and further the discussion to secure AI by design because we are very concerned that as we move forward to more organizations, just really

ubiquitously deploying AI, that we are going to have an even larger expanded attack surface and more of these challenges.

Mr. GARBARINO. So do you mind, Chairman?

Chairman GREEN. No.

Mr. GARBARINO. So that's my follow-up question. I mean, because you talked about AI Secure by Design. I have heard it multiple times now, specifically, you know, when it comes to legislation. You know, we are looking at how to regulate, and you have just talked about a study that said 40 percent of code written by AI is coming up with vulnerabilities or could have vulnerabilities.

You know, when Government takes action doing, you know, zoning, they look at an environmental study. You know, they look at the effects of what the project will do.

You know, we are looking at regulating AI and it has now been brought up to me twice in the last week how nobody is doing a cybersecurity review of what Congress is contemplating when we are talking about regulating AI.

It sounds like that is what you all are talking about here. Nobody is looking at whether the AI product is going to have data protections or cybersecurity built into it.

So I would love to hear more of your thoughts about how everything we have now, it is out there with, you know, Secure by Design. You have to go back and fix it. AI is still being developed. So what do we do?

Ms. Manfra.

General MCMASTER. Can I?

Mr. GARBARINO. Oh, yes.

General MCMASTER. Can I just defer to my palace on that?

Mr. GARBARINO. Yes.

General MCMASTER. Washed up generals should not be talking about all this technology.

But I will say quickly though there is going to be a tension between rapid model adoption and whatever kind of security protocol we put into place. We have the best AI models from what I have learned from people who know this business, but the friction and the difficulty is in adopting those models.

What the CCP's advantage is is that they can adopt those models much more quickly than we can. So I would just say whatever we do, maybe think in terms of incentivizing the kind of security but not delaying the adoption of these models.

Mr. GARBARINO. Thank you, General.

Ms. MANFRA. What truly will fit in and maybe I will kick it off here, is, on the one hand, we have to recognize that there is competition and we want American companies and American economic leadership in AI, and so we have to ensure that that is continued to be incentivized.

At the same time, AI has a lot of potential for improving our cybersecurity capabilities. There is a tremendous amount of noise that cybersecurity defenders have to deal with. I think you talked about this a lot. So using AI to be able to help them sift that signal out of the noise.

We have security operators that spend lots of time doing things that could be automated instead of, you know, taking that to the next level of critical thinking of what could be done.

So there is a lot of opportunity with AI to improve security. What I would just offer is so at Google we have put out what we call Secure AI Framework, which was based off of our own internal work in both leveraging AI for ourselves but also understanding and learning a lot of lessons about securing AI.

So we have put that out, and we are working and built a coalition with a lot of other companies for the use of secure AI and open-sourcing solutions to help organizations protect against some unique areas of AI that sometimes cross over also into safe use of AI. Recognize that.

A lot of AI security is still the same security. You still need to do the same things that you need to do in general, but there are some novel things for AI. So I would offer that the work that the coalition is doing and some of the standards that are attempting to drive through Oasis and other foundations might be a good place to start if you are thinking about what those standards should look like for AI.

Mr. CABLE. I would first like to start by really echoing Ms. Manfra's comments that AI is enabling tremendous innovation. We are here at Stanford. This hearing is on innovation. We are here in Silicon Valley. I live in San Francisco and see every day how AI—let's focus, for instance, in the role of writing software—is vastly changing how that looks.

I think we can reasonably expect if not today that within 1 or 2 years AI will be writing the vast majority of code that is in use. We can see how AI can accelerate building software for cybersecurity products. We are doing some of that ourselves, but also for scientific discoveries in many other fields.

I think there is a lot of new, exciting possibilities, but to the discussion here, we do have to recognize that much like humans writing code can introduce vulnerabilities, so can AI, and I think we have a really great opportunity to get in at the start, at the point when these models are being trained, at the point where these tools are just starting to take off, and build safeguards in place.

So I think, for instance, we are focusing particularly on the case of helping secure as companies are adopting AI for writing code and enabling them to write code 5, 10, many times faster, to have some guardrails in place.

To Ms. Manfra's point, both in terms of the security of AI systems, but also the vulnerabilities that AI can introduce, the vast majority of the time this is not going to be anything new. It is going to be the same classes of vulnerabilities that we have known about for decades, we have been struggling with for decades, and yet we have known how to prevent them at scale.

So I think this gives us really great opportunity to begin to put some of the action that, for instance, Google, other companies have really pioneered to root out entire classes of vulnerabilities and make sure that AI is designing software that is Secure by Design and is more resilient to these attacks from our adversaries.

Mr. GARBARINO. I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Swalwell for his time in questioning, and we're not really keeping a clock, Eric. So take all the time you need.

Mr. SWALWELL. Well, Mr. Cable, you mentioned that, you know, we are obviously at Stanford, your alma mater, and, General, I think you are affiliated now with this great institution. Could you speak to the role that the Federal support for technology has had on cybersecurity innovation, particularly as it relates to academic research?

If anyone else wants to add to that.

General MCMASTER. Well, obviously, the research programs at universities have been one of our greatest competitive advantages. Our ability to develop technologies but then spin those technologies out so entrepreneurs can take those technologies and put them into action in terms of real capabilities that give us our greatest differential advantage.

It is our innovation and then our ability to combine that innovation with our unbridled entrepreneurship, and so universities enable our free market advantages.

The other critical aspect of it is the development of human capital, and I think one of the most disappointing things that we have seen recently is the degree to which we have lost a lot of critical expertise within the Government, expertise that was developed in institutions like this that were serving with great distinction in the Government. Mr. Cable mentioned this already.

But then also, where there is a tremendous opportunity here in the Academy is to attract the best talent from within our country certainly, but internationally as well. So the impediments we have seen to bringing in, you know, the best minds and then to provide them with the kind of education that can help give us a differential advantage, and then of course, the other part of that is the visa process and immigration reform that would allow us to take advantage.

I think nobody is trying to immigrate to China, right? So this is one of our greatest competitive advantages.

So I am concerned. Of course, there are a lot of efficiencies to be gained probably in academia and research, you know, maybe too much overhead. I think reform is necessary, but certainly we do not want to give up that differential advantage in human capital, technology, and innovation.

Mr. SWALWELL. Thank you. Well said.

Does anyone else want to add to that?

Well, I have a practical question. As a parent to an 8-year-old, a 6-year-old, and a 3-year-old, when should our children start to be taught AI?

Are you thinking about this as an industry as you prepare for the work force?

Because I think the General is right. We want to attract the best and brightest around the world, but I still want to look my constituents in the eyes and say I am doing everything to make sure that your own kid is going to have the best shot to compete for that job as well.

So like when should we start to prepare our kids to use it?

Ms. MANFRA. I can start as the mother of a 13-year-old. I think I believe the approach to technology and cybersecurity in general is early awareness, and of course, you have to moderate within your own sort-of risk construct of the level of engagement that you

allow the young children to have, but helping them understand how they keep their information private, how these systems work so it is not just a black box for them is really important.

Also allowing them to learn about AI and what AI can offer them, but understand, and I think children at a pretty young age can understand some of these complexities, but helping them see both the benefits and the cons, I think, is really important.

So that is my personal experience. On the Google side, we invest a lot in educating and really trying to raise that next generation of computer scientists and security engineers all the way from elementary school through college, and so I absolutely believe it is really important.

Mr. SWALWELL. I do not know if you are like me, but I get fact checked by Alexa like 4 times a day by my 8-year-old.

Ms. MANFRA. Yes.

Mr. SWALWELL. He will ask me something and he will compare Alexa's answer to mine.

Ms. MANFRA. Yes. I tell him that he can do it as long as it is Gemini.

Mr. SWALWELL. Yes, right, right.

Mr. Cable.

Mr. CABLE. I would agree with that, and I would really add that at the core to a lot of this is this idea of digital literacy, and I think in addition to understanding AI, for instance, I think it is going to be more important than ever that children understand the basics of areas like computer science and can really begin to know how these systems work so that they are able to navigate them.

I myself started coding when I was 11 and really had a journey teaching myself how to build websites and apps and saw a lot of the potential in computer science.

To Ms. Manfra's point, I think there is also a critical area where we need to pay attention to our current and future software developers. One area that I will note, and I saw this when I was an undergraduate at Stanford, is that across the top 20 universities in computer science today in America, not one of them requires students who are getting a computer science degree to take a security course or to learn about security.

If we think about security being really core to the future of software development, as we have discussed in this hearing today, I think it is essential that current and future software developers know a thing or 2 about security, much like we would expect, say, civil engineers to understand how to ensure that bridges can be built securely.

So I would encourage this committee to explore how we can really make sure that computer scientists are considered a core part of the software and cyber work force and to ensure that they have the baseline understanding of security.

Mr. SWALWELL. Great. To all of the witnesses, what is your assessment of the current state of preparedness in the United States for quantum threats, and how can we expedite efforts to prepare for quantum computing, particularly as it would relate to, you know, decrypting our data?

We will start with the General.

General MCMASTER. I mean, maybe just a general comment.

China is attempting to surpass us in quantum technologies. You may say they have already done that in capacity, but not yet in capability. So obviously, it is very important for us to invest in it because we can use those same kinds of capabilities to defeat deencryption.

But I will turn it over to the real experts here.

Ms. MANFRA. I will not pretend to be an expert in quantum computing, but what I can say is——

Mr. SWALWELL. Well, I guess, how is Google preparing for?

Ms. MANFRA. There is a need for people to take this more seriously. There is the post-quantum crypto world is going to be very real soon. If I recall correctly, the NIST–NSA time lines to make sure that you have adopted post-quantum crypto is 2035, I believe, and I still think that is a good target.

Google has been investing a ton in both post-quantum cryptography capabilities, but also quantum computing. We just released a paper a couple days ago about this.

The thing though is people think, well, that is 10 years away, but it takes a while to implement these capabilities, and so I would just encourage organizations and this committee as you are looking at this is it is not just something that an organization can figure out in 6 months.

They need to be taking it seriously. They need to understand what their capabilities are. We have been working on it and implementing post-quantum crypto capabilities for a few years now, including in our internal communications. We do have some capabilities that we offer customers as well.

But I would say hard to make a broad estimate on preparedness, but I would say generally we do need to take it more seriously as a community.

Mr. SWALWELL. OK.

Ms. WHITMORE. I would echo Ms. Manfra's comments.

Just in terms of Palo Alto Networks, our approach has also been for years being concerned about what happens with post-quantum ability to decrypt information that today is protected.

So we have focused on that particularly with our network security products as well as our implant security products that today, you know, are able to withstand what we believe to be, you know, post-quantum attacks moving forward and then also offer some options for our clients as well to help them implement those strategies.

But you could not have said it better, I think, in terms of the 2035 deadline. I think it is, you know, far too distant in the future. I think we need as a Government, in particular, to be attacking that as if it is more near term.

Mr. SWALWELL. Thank you.

Ms. Whitmore, you had mentioned support for the JCDC bill that the Chairman and I were able to pass together out of the committee last year. Can you speak, also Ms. Manfra, both of your companies are a part of JCDC; can you just speak to any reforms that you would like to see or, you know, what we could do to make it more agile and, you know, a better Neighborhood Watch-like program?

Ms. WHITMORE. I think your earlier comments commented on the need for, you know, very effective two-way street, and when we see information sharing of any kind, whether it is between public and private partners or smaller industry-led groups, the challenge is oftentimes organizations who provide a lot of information and then organizations who do not share as much, and the information in those types of settings is only as effective as it is incredibly actionable and contextualized and timely.

So I think the need to further encourage that effective sharing is on, you know, a two-way street and make sure that from the timeliness perspective the types of data we are focusing on are going to drive the outcomes we are looking for.

Mr. SWALWELL. Thank you.

Ms. MANFRA. I would agree. I would add that it is a real opportunity to focus on, you know, we have been talking a lot about baseline standards and raising the baseline, but there is this other really important area of the sectors and, you know, that higher-level threat.

So CISA, I think, has a real opportunity to deeply understand national risk and, using the JCDC, to bring those private-sector and Government entities together that have unique capabilities to reduce those risks.

I think it is important to be very focused, right? We talk a lot about information sharing, but information sharing for what purpose? Just generally reducing cyber risk is too broad.

So what specifically are we focused on? What specific threat are we working to reduce the risk of? Which sector are we focused on?

There are a lot of companies participating that have a lot of amazing intelligence and, you know, the Government brings a lot of amazing intelligence, and so how do we focus that work more on disrupting those highest threats and reducing those most significant risks to the country?

I think that is a really big area to focus on.

Mr. SWALWELL. Thank you.

Chairman, I yield back.

Chairman GREEN. So I know there are probably some other questions. You have a few and Mr. Swalwell might generate 1 or 2 as we are continuing. I did want to say a couple of things and had a question. I will let Mr. Garbarino ask 1 or 2, and then if 1 pops up, we have some time.

Are you all doing OK? Does anybody need a break?

All right. We talk about this economic model, and I mentioned it where we talked about the victim versus the villain and there being a very low cost of entry for the villain and a very high cost.

I think there is another economic model, and that is that first to market, which results in vulnerabilities, and I get the competitive advantage of first to market. I ran a health care company and I always wanted to beat my competitor to market because it did give you a financial advantage.

But I am just making an observation here. This is something that we have to figure out, and I do think liability has to play a role in it.

Here I am an ER physician suggesting that liability is a good thing. My lawyer buddies' jaws are on the floor, but, no, I do be-

lieve that it is the path or a path, certainly a course of action that we have to consider.

One of the questions that kind-of came to my mind as I am listening to the witnesses, and we have got this incredible panel here, someone from academia now but who spent a lot of time in the military. We have got 2 of our Nation's greatest companies, I mean, really.

We have got a start-up, a guy who was in Government and who is now starting up, a young entrepreneur.

So the question comes to mind about education and the talent pipeline, and my question is, you know, we train cyber folks in the military. I think you helped, if I remember this correctly, start Army Futures Command and get all that going.

We educate cyber professionals. In the civilian sector, we educate cyber professionals. You know, in the military to get people excited about the military, we have these simulators that go around, and you have got a young 12-year-old who hops in and flies an Apache helicopter. It is the coolest thing. It gets them excited at a very young age.

Now, what are some ideas on how we can do that for the cyber space and how can we collaborate on military education and cyber, our military guys and our academic centers, in preparing sort-of this work force of the future for cyber?

You know, anybody, all of you feel free to answer. No. 1, recruiting, and No. 2, how do we work together to collaborate to get to where we need to go?

Mr. CABLE. I am happy to kick this off, and thank you, Chairman, for the question.

I would maybe start with, to your point that it is not just about the victims or the villains but really that the vendors, the manufacturers of software products have a key role to play here, and I think we can extend that to the cyber work force, recognizing that cybersecurity professionals alone are not going to be able to solve the cybersecurity problems of today, and that is because we really need to work back to the point where software is developed.

So what I was saying earlier that we need to ensure that every current and future software developer has a solid understanding of the security baseline and knows particularly as they are using more and more AI tools, writing less code themselves and more so instructing AI assistance to write code, that they know how to identify vulnerabilities and to produce more secure software.

But that is also an area where technology can help and that we can leverage artificial intelligence, for instance, to help educate software developers to help flag security issues as they pop up and make sure that ultimately we can really build products that are more secure by design.

I have seen first-hand the impact that really real-world experience can have when it comes to getting into cybersecurity. When I was 15, I found my first vulnerability in a Bug Bounty Program, participated in many more, have reported vulnerabilities, too, to companies like Google, and there are many companies out there today that embrace security researchers with open arms. The U.S. Government does as well.

That is how I found my path into working in the U.S. Government after placing first in the Hack the Air Force competition.

So I think we really need to build up more of these initiatives as well to get young people excited, to get young people participating.

When I came to Stanford my freshman year, I helped create a Bug Bounty for Stanford and then spent the following several years identifying vulnerabilities in Stanford systems. So the more we can do to really give young people hands-on experience and cool technical challenges, I think we can really motivate people to join the cyber work force.

Chairman GREEN. I hope they reduced your tuition for that.

[Laughter.]

Mr. CABLE. It certainly helped.

Chairman GREEN. Yes, good.

Ms. MANFRA. I think that is so well said, and I would also just add that I think Google has proven that you do not have to sacrifice velocity for security.

So it is, to what Mr. Cable was saying, a lot of this comes back to, do the software developers have the tools and the practices that allows them to code in a secure way?

Do you, you know, make security hard for your developers and your users or do you innovate in tools and capabilities that make it a pleasure to develop on your system, in addition to it being secure and reliable?

So I think we need to be looking at more of those instead of continuing in these sort-of false choices that you have to either have velocity or security.

It does take a different mindset, and sometimes that might need to be imposed externally on organizations, but I absolutely think it is possible.

On the other side, on the work force, I think there is both developing a work force of individuals who are going to be focused on cybersecurity, absolutely, and entice them into the Government for as long as we can keep them there. Government has got so many interesting problems that people cannot find outside in the private sector. So I think there are a lot of opportunities to do that and continue to invest there.

But I would also say we should not just focus on teaching cyber to cyber professionals. Lawyers need to understand it. Doctors need to understand it. Teachers need to understand it.

So building more interdisciplinary programs, organizations like Stanford and others throughout the country are doing this, but bringing people together so that a lawyer can understand the technical aspects of a situation in cybersecurity. An engineer can understand even potentially some of the legal aspects.

So cybersecurity, I think, is really important from an interdisciplinary perspective and being able to bring these different disciplines together, whether that is an anthropologist. We have hired anthropologists who bring like an amazing viewpoint into this area, or making sure our engineers understand secure coding practices. I think there are lots of opportunities in that space as well.

Chairman GREEN. You generated a thought, and I do not know. Maybe this is what you were saying and I just thought it was novel

in my brain, but you know, we have History 101 when you go to college. It is required. I mean most colleges require it, but there is a required basic curriculum to get an undergraduate degree at just about every university.

I mean, why not a Cyber 101 a part of the required curriculum at universities? If you are going to school here, you know, you are going to take Cyber 101.

Ms. WHITMORE. I certainly second or third the commentary that has been said. I think it is critical that we continue to work with universities to shift the curriculum.

Mr. Cable mentioned that, you know, just as recently as when he had received a computer science degree, security classes were not mandatory.

I personally work with both Duke University as well as University of San Diego, which was my undergraduate alma mater, in their security programs, and so we are actively shifting a lot of the curriculum to ensure that those programs include security.

I think the cross-disciplinary commentary is critical. It is certainly critical in business when we see, you know, these attacks occur.

I think, No. 2, it is going to make it easier for people to cross-train into this work. So the Cyber PIVOTT Act is a great example of that where you are not just looking at traditional 4-year degrees but shortening those time frames.

No. 3, I think we must create competition, and that is not just, you know, college competitions or Hack the Air Force, which are great, but you know, our adversaries are creating elementary school competitions where cyber competitions are as critical as, you know, ice skating and football are.

So I think that is an area that we really need to look at bringing into.

Then fourth I think is with technology. I do not think the right approach is going to be for us to only look at those as a people work force challenge. We have got to be able to leverage technology in a particular AI to start closing that gap in order to make the work that people are doing, really make them feel like they are having more of an impact or taking away some of the repetitive tasks that drive people out of the career field and creating new opportunities to have impact.

Chairman GREEN. General, I do not know if you want to comment on collaborating military and civilian universities together on this issue, but that is the one piece of this that has not been commented on.

General MCMASTER. Yes. Hey, thank you, Mr. Chairman.

I would. When I first arrived here in 2018, just having left Washington, I was struck by the degree to which there was a degree of suspicion really almost between the public sector and the private sector. It was the post-Snowden kind of hangover, and Rashawn and Amy Ziebart and I put together what we called a Tech Track 2 dialog, which is now going strong.

I have seen a tremendous shift in attitude. I think maybe almost especially after the massive re-invasion of Ukraine in 2022, a recognition that there are really still real threats in the world that we have to be concerned about.

So the attitude, I think, is right to maybe take us to the next level. One of our first Tech Track 2 dialogs we focused on getting pledges from the private sector and from the military services to vastly increase their exchanges. That happened, and I think that momentum has continued.

I think what the Trump administration is doing now, the Department of Defense to make it easier for people who have these extraordinary capabilities to get direct commissions in our services and continue to contribute to their companies but also contribute to security within Government.

But, of course, we still need really some of our best people, you know, in Government, and we have them already. I am concerned about sort-of this shift in the perception of service that like it is not quite as hip as being, you know, out here in Silicon Valley.

Well, you know, actually the real hard problems, a lot of the real hard problems are in Government, and it is exciting and challenging. So I think what we have to do is talk to our young people about the tremendous rewards of service and then make that gateway easier with internships, which I encourage our students here to engage, and many of them have done that. Many of them are now working for the Government in many capacities and self-actualizing and feeling like they are making a contribution.

So it is internships and exchanges. These are things we can measure, but also I think the military model of the Reserves is really critical here. We have seen this happen now in terms of our cyber capabilities within cyber units. One of them is at Moffett Field right here, and it allows some of our top people to also contribute in uniform and then to go back to their private sector.

So I feel good about that. There are a number of programs here that I have highlighted inside of my statement for the record. So I will not go through all the details, but I mention Tech Track 2. There is also a Tech Policy Accelerator here at the Hoover Institution where we are bringing together Government, private sector, and figuring out these policy solutions, recommending them.

I hope that you will consider us an extension of or your staffers will consider us an extension of your staff and we want to help with this.

Also in terms of educating people, there is the Stanford Emerging Technology Review, which is meant to make the critical technologies, many of which we are talking about here, accessible to the American public.

Then in the area of education, I will provide you some examples, you know, because education in our country is very decentralized. There are some really best practices on getting young people involved in and educated in this area of cybersecurity. Many of them are feeding high school graduates like in the San Jose area directly into companies here in Silicon Valley.

So I feel optimistic about it. I think everybody wants this to work.

Then the last comment I would make is on education, Congressman Garbarino mentioned already his trip to Estonia, this whole idea of like the digital citizen. I mean, Estonia is a pretty small country compared to ours, but there are best practices there that I think could be scaled up as well.

Chairman GREEN. Mr. Garbarino.

Mr. GARBARINO. Thank you, Chairman.

Chairman, I wanted to ask you. You were National Security Advisor back in 2017, 2018. I know you cannot get into specifics, but can you talk about the benefits of the Cyber Information Sharing Act of 2015 and why you think it is probably necessary that it gets renewed, just the importance of that collaboration?

Chairman GREEN. Yes. It is vitally important. I mean, there is no way. As we have already mentioned, you cannot have all this expertise in-house across the private sector and all these companies that touch critical infrastructure. It is important that when there are breaches of security that our Government is aware of those immediately so we can work together not only to spread the warning about that, but to help develop those solutions.

So I think that was an extremely important development. I would also say in that same period, 2017 to 2018, we made some adjustments which I think really helped us tremendously along with inspired leadership at NSA under General Nakasone to be much more responsive in recognizing that a good defense requires a good offense.

So whereas our private-sector companies say we can defend all day, you know, but even if you have the best layered defense, if you have got, you know, the least privilege in place, if you are Secure by Design, they are still going to get at you somehow.

So every good defense has to allow you to shoot down the arrows coming at your service area, but also to go in and kill the archer, and you can only really get help in doing that by a good partnership and reporting between the public sector and the private sector.

Mr. GARBARINO. If any of the other witnesses want to talk about the importance of CISA 2015 being reauthorized, it is great to have it for the record so when we go to redo it we have all of these people saying wonderful things.

Mr. CABLE. I would certainly agree, speaking from my time at CISA. I can attest to the importance of making sure that the private sector can collaborate closely with CISA and protections like in CISA 2015 are essential in making sure that private companies feel comfortable providing that information.

One of these initiatives that I will mention is the preransomware notification initiative that I had the privilege to assist with when I was at CISA, and that is one instance where security researchers are sharing tips with CISA of impending ransomware attacks such that CISA cannotify critical infrastructure owners and operators ahead of those attacks to prevent them from occurring.

CISA has prevented thousands of incidents through the preransomware notification initiative, and this really is only possible due to the trust that CISA has built with security researchers, with private companies, and is enabled by Acts like the 2015.

So I do believe that is essential that this gets renewed.

Mr. GARBARINO. Great. I do have a follow-up question for you, Ms. Manfra, but if you all want to talk about CISA real quick, that is fine.

Ms. MANFRA. I would just join and say I agree that it is important to reauthorize.

Ms. WHITMORE. Also for the record, Palo Alto Networks is in support of CISA 2015 as well.

Mr. GARBARINO. Wonderful. The second part of our title of the hearing was streamline compliance, and, Ms. Manfra, you brought it up in your opening testimony about compliance reciprocity. I mean what do you mean by that?

It is something that the committee and the Chairman is great. I think he has got the whole committee working on a regulatory compliance memo that is going to be released hopefully soon, but it has been a big focus of the committee.

Chairman GREEN. Harmonization.

Mr. GARBARINO. Harmonization, yes. Harmonization, but it is still part of it.

Ms. MANFRA. Yes. Well, absolutely. So from a harmonization perspective on the regulatory side, both you know for what we see and for our customers, it is a complicated area that people have to operate in.

So being clear on, you know, thresholds and requirements and making those common as much as possible and then having that common standard is important.

The specific thing that you were asking about with the reciprocity is ensuring that if, you know, you have programs like FedRAMP certification regimes for civilians, you have DOD and their impact levels, and other emerging certifications, we want to make sure that there is reciprocity.

It is a fair amount of investment for companies to go through these processes, and so you want to make sure that if you go through one and it is the same standard, that that is then recognized by those other programs. That is what I was referring to.

Mr. GARBARINO. OK. Very cool. Thank you very much.

I yield back, Chairman.

Chairman GREEN. Well, I deeply appreciate all of you for coming today.

You know, the unipolar moment is gone, and we sit in a battle between, you know, 2 countries really, but I mean there are other players that are very important, and I think it is about 3 things.

I think it is about talent management. I mean, if you go and study Confucianism, neo-Confucianism, and Sun Tzu and all of that, I mean, they had these tests for Government service and it is all about talent management.

For us it is talent management, and in the cyber space, that is really, really very important.

It is also about alliances and friends. When the world becomes a bipolar world, and we have a lot of work to do there, and we have to be very careful about some of the things that we are doing in that regard.

Then it is about our economy and how we make our economy powerful. You cannot buy tanks. You buy tanks with GDP, and so you know, how we spend and how we work as a Government, all these things are very, very important.

We are doing our best to juggle all of these balls and keep Government out of the way and partner where we can. But in this space, in the cyber space, I am very focused on harmonizing and getting Government out of the way and getting to a vision where

compliance is really done in real time with AI, and no human has to put a single effort toward it because companies like your-all's can do it for us instantaneously, and all that effort and energy in the private sector going toward checking the box goes toward real cybersecurity and protecting those entities.

So that is something I am very passionate about and all these other things we have talked about today.

So, again, thank you.

What we are going to do now is take a break, and I know there are probably folks in the room who will be joining us for the next phase of this, but the next phase is really about identifying the, you know, critical components so that we can develop courses of action.

What can we do? Do we want to outlaw ransomware payments?

I threw that out there not because I was convinced that is the right thing to do, but I mean, we have to have these dialogs. When we sit down and war plan a battle, whether it is taking a hill or, you know, destroying a bridge or denying an enemy this, we sit down and we just brainstorm. I mean that is what course of action development is. It is what could we possibly do.

That is what I hope to do in the next section, is sit down and ask some hard questions. What should compliance really look like?

What should we not be worried about and things like that?

So I am hopeful that our next session will walk away with action steps for us and for yourselves.

So, again, thank you for being here today. The committee now stands adjourned.

[Whereupon, at 3:40 p.m., the committee was adjourned.]