Written Testimony of:

Wendi Whitmore
Chief Security Intelligence Officer
Palo Alto Networks

Before the:

Committee on Homeland Security
United States House of Representatives

Titled

# "Innovation Nation: Leveraging Technology to Secure Cyberspace and Streamline Compliance"

May 28, 2025
2:00 PM

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 nine 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 policymakers appropriately cultivate a robust and ongoing 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 of 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 policymakers 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 cyberattacks.

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 cyberattacks. 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% 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.

- Cyberattacks Are Moving Faster than Ever. Attackers exfiltrated data in under five hours in 25% of incidents in 2024, which is three times faster than in 2021. What's even more alarming is that in one in five cases, data theft occurred in under one hour.

- AI Is Accelerating the Attack Lifecycle. 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 cyberattacks, responsible for 23% of all initial access. Fueled by generative AI, phishing campaigns are now more sophisticated, convincing, and scalable. Inclusive of phishing, 44% of the attacks we investigated in 2024 involved a web browser – heightening the importance of browser security.

- Complexity Is Killing Security Effectiveness. In 75% 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% of incidents, attackers exploited three 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% of cyber incidents involved cloud environments, with 21% 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% 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 six 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 *one* 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 two hours, *with ~60% of customers under 10 minutes*.
- Fivefold increase in incident close out rate.
- Fourfold 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% of enterprises are already leveraging AI tools. This is expected to grow to 96% 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% of employees currently use AI apps without permission in their enterprise, 80% 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 timeline 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 policymakers 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.

Statement of LTG H.R. McMaster (U.S. Army, retired)
Senior Fellow, Hoover Institution, Stanford University

Before The House Committee on Homeland Security's
Subcommittee on Cybersecurity and Infrastructure Protection
Silicon Valley

Field Hearing on "Innovation Nation: Leveraging Technology to Secure Cyberspace and Streamline Compliance"

28 May 2025, 2:00pm 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 cyberattacks 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 cyberspace 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 cyberspace has grown due to AI advancements and the increased connectivity of physical objects to cyberspace. 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 cyberspace 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 cyberattack 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 cyberattacks 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 EU 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, fifty-two ports in thirty-four 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 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

[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.

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 cyberspace 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 cyberspace 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 cyberspace 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 cyberspace.

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.

**Testimony of Jeanette Manfra**
**Senior Director, Global Risk and Compliance**
**U.S. House Committee on Homeland Security**
**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 lifecycle — 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 dialogue 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.


Written Testimony of Jack Cable
CEO & Co-Founder
Corridor

Before the U.S. House Committee on Homeland Security

Hearing on
"Innovation Nation: Leveraging Technology to
Secure Cyberspace and Streamline Compliance"

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 firsthand how insecure software can jeopardize our public safety, particularly as both nation-state actors and cybercriminals 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 cyberattacks on our power grids, water systems, telecom providers, and more.

But these attacks are not inevitable, nor unpreventable. The vast majority of cyberattacks 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.

---

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

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 about 30-40% 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 tradeoff 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 cyberattacks, 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

[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

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 U.S.

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 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.

[6] https://www.lawfaremedia.org/article/advancing-secure-by-design-through-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.