Written Testimony of Kemba Walden

United States House Committee on Homeland Security
Hearing on "Unconstrained Actors: Assessing Global Cyber Threats to the Homeland"
January 22, 2025

Chairman Green, Ranking Member Thompson, distinguished members of the Subcommittee, my name is Kemba Walden, and I am the President of Paladin Global Institute (Paladin), a think tank committed to ensuring that secure critical infrastructure and the safety of people online remain core to sustainable technological innovation. I also serve as a co-chair of Aspen Institute's U.S. Cybersecurity Group, which published cybersecurity policy recommendations for the new Administration, some of which are reproduced below, based on the collective experience and expertise that membership gained over decades of experience in the public and private sectors.

Prior to Paladin, I served as the acting National Cyber Director and the first Principal Deputy National Cyber Director in the Office of the National Cyber Director in the Executive Office of the President. Before that, I was an Assistant General Counsel in Microsoft's Digital Crimes Unit (DCU), where I led the Ransomware Analysis and Disruption Program. I also spent a decade in government service at the U.S. Department of Homeland Security (DHS) in several attorney roles, specifically as the DHS lead for "Team Telecom," the lead attorney for the DHS representative to the Committee on Foreign Investment in the United States (CFIUS) and then as a cybersecurity attorney for the Cybersecurity and Infrastructure Security Agency (CISA), and its predecessor.

Over the course of my career, I've witnessed the evolution of global cyber threats, new approaches to exploiting vulnerabilities in technology, and our responses to them. There are three types of cyber threats – nation state actors, criminals, and insider threats. And there are two evolving types of vulnerabilities - the pace of technological advancement, and the status quo of business processes. The impact of these threats and the creativity and sophistication with which malicious are exploiting vulnerabilities is considerable.

The world is in a state of flux. The risks are too high to continue to take a tactical approach to responding to these threats individually. Faced with this strategic context, we must continue to pursue a more resilient and defensible infrastructure that is aligned with our values. A sustainable and successful effort against these threats will require a whole-of-government strategy executed in close partnership with the private sector, our allies, and international partners.

Over time, we've matured our governance and developed strategy, but there's much more to do. In this testimony, I first describe three types of global threats and two pernicious vulnerabilities—and second, I offer governance, skilling, and technological solutions to mitigate the resulting risks.

In this testimony, I will leverage the expertise gained through the work of Paladin Global Institute, its insight into various markets, and my experience through Aspen Digital and previous roles, to provide an overview of the threat landscape and provide recommendations I believe this subcommittee may find relevant as it continues to consider responses to these global cyber threats. Paladin Global Institute leverages its global reach and deep bench of cutting-edge thought leaders and policy experts to protect global critical infrastructure. Paladin encourages both (1) operational opportunities to mitigate cyber threats and vulnerabilities and (2) policy solutions for sustainable cybersecurity and cyber safety improvements.

A. The Evolving Landscape of Global Cyber Threats and Vulnerabilities

1. Nation-State Actors

As the world bears witness to the transition to a new Administration and a new Congress, our adversaries are considering exploiting vulnerabilities in the seams created by the transfer of power. It is in these transitions where pernicious threats thrive, and vulnerabilities loom largest. To advance their own geopolitical standing in the world and to impact the balance of alliances, nation state threat actors aim to strike when the United States is at its most vulnerable. These threat actors use diverse methods to achieve their geopolitical aims, but they share common goals. They each need for the United States to appear weak and off-balance, and they've learned that there's opportunity during times of transition.

These threats are coalescing around common goals. This month, Russia signed a treaty with Iran to expand economic and security ties between the two countries. Last year, North Korea also signed an agreement with Russia to provide military assistance in times of war. In 2022, China and Russia announced a formal partnership announcing that there are "no limits" to areas of cooperation between the two countries. These reported alliances inform the dynamic nature of global cyber threats.

Russia

Russia uses cyber operations as a foreign policy lever to shape other countries' decisions, focusing on cyber operations to gain advantage in the Ukrainian war and the region, but continuing to target critical infrastructure in the United States. When the Biden Administration was transitioning into office, it did so in the wake of the Russian state-sponsored breach of the SolarWinds Orion platform. This supply chain attack was novel in its approach, and unprecedented in its reach. Russian-backed cybercriminals then to breached Colonial Pipeline and held it for ransom. The world then watched the subsequent run on gasoline across the East Coast of America and learned that cyber has power in the real world. Russia's Federal Security Service has long-standing ties to national cyber criminals and indigenous hacktivist communities. Because of their relationship with the government, the government tacitly permits criminals to operate, shielding them from U.S. law enforcement.

The People's Republic of China (PRC)

As noted in The Office of the Director of National Intelligence's 2024 Annual Threat Assessment, "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks." As the People's Republic of China (PRC) seeks annexation of Taiwan, with U.S. Adm. John Aquilino, Head of U.S. Indo-Pacific Command, noting "all indications" point to the Chinese military being ready for a potential invasion of Taiwan by 2027, the PRC has moved to prepare the battlespace. Long gone is a China simply focused on IP theft; we've now witnessed China snooping on telecommunications networks (i.e., Salt Typhoon) and prepositioning in U.S. critical infrastructure to enable disruption operations in preparation for a future military conflict with the U.S (i.e. Volt Typhoon).

The most recent revelations about China's massive cyberattacks on U.S. critical infrastructure and telecommunications networks demonstrate the increased sophistication of PRC threat actors, and the expansion from espionage to potential disruption or destruction activities. Although the PRC threat actors used to be known for "smash and grab" cyber intrusion, they've moved to a new era of stealth cyber intrusion, with the PRC exploiting legitimate privileges in private sector systems not only for espionage, but more importantly to hold our critical infrastructure at risk. Through an operation, named Volt Typhoon, we discovered that the PRC were "living off the land" in our infrastructure to evade our detection technologies. Over time, the PRC gained sophisticated knowledge not only of our technology but of the governance structure through which we secure that technology, forming creative opportunities for exploiting new vulnerabilities.

One additional known PRC penetration strategy is through PRC investment in U.S. critical infrastructure. Working often through creative investment vehicles, the PRC took a strategic approach to eventually holding our infrastructure at risk while the United States took a tactical approach to blocking transactions that raised national security concerns. As your Committee found in an investigation, this includes investment in the maritime industry, with two-PRC state-owned enterprises controlling portions of five U.S. ports. Notably, the PRC is outpacing most national investments in emerging technologies. According to some reports, the global investment in quantum technology is over $40 billion, with the PRC driving approximately $15 billion in investments whereas the U.S. is investing just under $5 billion

As early as 2012, the House Committee on Intelligence warned that "the United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies" and further recommended that "Committees of jurisdiction in the U.S. Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure." In response, at the direction of Congress, the Federal Communications Commission established the Supply Chain Reimbursement Program to reimburse small providers of advanced communications services for expenses related to the removal and replacement of communication equipment and services provided by Huawei or ZTE. More work remains to be done to remove Chinese equipment from our critical infrastructure, including TP-Link consumer routers in the U.S. which have been used to launch cyber-attacks via a Chinese hacking entity that maintains thousands of compromised TP-Link routers. The fact that TP-Link is dumping routers in the US market below a profitable point has enabled them to move from 8% of the market to 60% in only a few short years. The PRC is playing the long game for an operational and strategic advantage.

Iran

Iran seeks dominance in the Middle East and conducts influence operation in the U.S. to include targeting U.S. elections. Just this summer Iran's Revolutionary Guard Corps-affiliated cyber actors targeted the Trump campaign, in efforts to erode confidence in the U.S. electoral process ahead of the November presidential election. In addition, we have seen Iran-based cyber actors enabling ransomware attacks and using brute force to compromise U.S. health care and other critical infrastructure providers.

Democratic People's Republic of Korea (DPRK, a.k.a. North Korea)

The Democratic People's Republic of Korea (DPRK) seeks the survival of the dynasty and to "reunify" the Korean peninsula under their terms and vision. Cyber operations are a main source of funding for the government which get around U.S. and international financial sanctions. In the earliest days of the Biden Administration, as blockchain technology was maturing and the virtual currency system built upon that technology were gaining in popularity, the DPRK found opportunities to exploit them for financial gain. Initially, the DPRK used ransomware to obtain virtual currency, but they later learned that exploiting vulnerabilities in blockchain technology and stealing virtual currency from cryptocurrency exchanges is far less expensive. We have also seen an uptick in DPRK targeting of critical infrastructure to steal technical information and IP to further its nuclear ambitions.

2. Cybercriminals and Fraudsters

The proliferation of cybercrime presents an escalating threat to our national and economic security. As reported by the FBI, criminal activities ranging from business email compromise, investment scams, ransomware, and fraud resulted in potential losses of over $12 billion in 2023. The General Accountability Office estimates that cyber fraud costs the U.S. federal government between $223 billion and $521 billion every year. Organized criminal groups have developed sophisticated ransomware operations impacting the operations and availability of critical infrastructure, including healthcare facilities, and government institutions. Of particular concern are the emerging trends of criminal networks recruiting and exploiting minors for cyber operations, creating both a security and societal challenge, and the proliferation of ransomware as a service, allowing less sophisticated cyber criminals to launch attacks at a lower cost. An insidious through line across many of these nation-states and cyber criminals is the abuse of network access and privilege, with threat actors stealing credentials through phishing attacks, social engineering, and malware.

Ransomware has evolved into a highly lucrative business model, with threat actors using advanced intelligence collection to shape ransom demands. Once criminal actors break into a network, they may access and study their target's financial documents and insurance policies, and research the penalties associated with data breach laws, to better inform their eventual ransom demand and negotiating position. Leveraging this significant intelligence gathered on victim companies, the criminal actors then launch their ransomware attacks, identifying what they regard as an "optimal" ransom amount. These criminal actors extort money from their victims, not only to unlock systems but also to prevent public disclosure, making significant money from data theft and double extortion, and deploying thousands of instances of malware across thousands of victims.

As cybercrime has evolved to more enterprise-like operations involving multiple players, countering these efforts requires a multi-stakeholder and global approach. The private sector and the U.S. government have engaged in and experimented with technical and legal models, globally, to disrupt and dismantle cybercrime infrastructure. Efforts to date illustrate that a collaborative multi-stakeholder approach – sharing actionable information and leveraging the combined capabilities of the private sector and the government – yields the best opportunity to disrupt cybercrime quickly and at scale.

Paladin's direct experience with technology companies engaging in public-private partnerships has shown how potent collaboration can be. One technology company's facilitation of many hundreds of FBI victim notifications had an impact far wider than just protecting the notified victims. In one engagement, the company intercepted an attack against an IT provider with over 600 large financial institution customers. The threat actor was planning to sell access to a ransomware affiliate who would then attempt to encrypt the IT Provider's customer networks, creating a catastrophic impact on not just the victim's business, but its many customers. Public-private partnerships, when scaled up as in this case, can disrupt the criminal supply chain, thereby making it more difficult for ransomware affiliates to successfully find and attack victims.

The cybercrime ecosystem is dynamic and massive, but the Federal government has done incredible work to hold these malicious actors accountable. The National Cyber Investigative Joint Task Force, law enforcement agencies, U.S. Cyber Command, the National Security

Agency, and other elements of the intelligence community have led multiple initiatives to increase the speed and scale of disruption operations, coordinating joint, sequenced disruption campaigns with international partners. Sustained efforts, and investments, in these programs will continue to defend the Nation and our critical infrastructure from ransomware threats.

3. Insider Threats

The increasing globalization of the job market, rise of remote work, and need for highly-specialized skilled workers provides global adversaries—specifically the DPRK and the PRC—an opportunity to creatively target U.S. companies' sensitive intellectual property (IP), high-tech research and development (R&D), and financial assets. Information Technology (IT) workers often have privileged access to systems. So, while today they may just be a source of hard currency (and occasional R&D), they could use their positions of trust to conduct more conventional cyber operations.

Since at least 2022, information technology (IT) workers from the DPRK have been fraudulently obtaining remote employment at unwitting companies in the United States, including at Fortune 500 companies across a variety of industries. DPRK threat actors use U.S.-based job search sites to seek employment with U.S. companies and use stolen U.S. citizens identities to gain employment. This scheme often requires the assistance of other U.S. individuals as facilitators to help the DPRK workers appear to be in the U.S. and move money and IP out of the U.S. These works, some of whom live in China and Russia, provide a critical revenue stream that helps fund DPRK economic and security priorities and helps the DPRK gain access to sensitive IP and R&D. These fraudulent employees put U.S. companies at risk of violating U.S. and international sanctions and put IP and sensitive data at risk.

Similarly, Chinese intelligence services abuse U.S. student and work visas to gain access to critical technology at U.S. companies and universities that require highly technical and skilled workers to fill critical technology roles. For those U.S.-trained Chinese nationals who otherwise cannot lawfully stay in the United States upon completion of their studies, the PRC benefits from the talent and skills and knowledge of those students when they return. Intellectual property theft from U.S.-employed or trained Chinese nationals poses a significant risk to the private sector and academia, particularly amongst the defense sector and emerging dual-use civil-military technologies, such as Artificial Intelligence (AI). In fact, approximately 60% of all FBI trade secret theft cases involve a nexus to the PRC. For example:

- In 2018, Chinese state intelligence actors used a U.S.-based job search site to target and clandestinely recruit a former US Intelligence Community employee.
- In 2019, a U.S.-based Chinese national pleaded guilty to stealing over $1 billion in petroleum research and development from 2017 to 2018.
- In 2020, People's Liberation Army Lieutenant Yangqing Ye falsely posed as a student to enter the US on a J-1 visa. While posing as a student, Ye conducted biomedical research

at Boston University, assessed US military websites, and exfiltrated sensitive documents and information back to China.
- From 2022 to 2024, US-based Chinese national employee exfiltrated sensitive company proprietary AI technology and research to two PRC-based startups.

4. Technological Acceleration

The rapid pace of technological advancement, while offering tremendous opportunities, also presents significant security challenges. As innovations in fields like AI, quantum computing, and biotechnology emerge at an unprecedented rate, they bring both exciting possibilities and potential vulnerabilities. It is in the seams where innovative technologies are integrated into legacy IT systems, that our adversaries find exploitable opportunities.

As stated in the 2024 Report on the Cybersecurity Posture of the United States and 2024 Annual Threat Assessment, these technological advancements can enhance our capabilities in various sectors, from healthcare to transportation, but they also create new attack vectors for malicious actors. The interconnectedness of our digital infrastructure means that a single vulnerability can have far-reaching consequences, making it crucial to stay ahead of potential threats.

We must shift from reactive to proactive security postures to address emerging threats from quantum computing, AI, and other transformative technologies. This paradigm shift requires a fundamental change in how we approach security, moving away from simply responding to threats as they occur to anticipating and mitigating risks before they materialize. For instance, the development of quantum-resistant cryptography is essential to protect sensitive data from future quantum computing attacks.

Similarly, leveraging artificial intelligence and machine learning for threat detection and response can help identify and neutralize sophisticated cyber threats more efficiently. Proactive security measures also involve continuous monitoring, threat intelligence sharing, and regular security assessments to identify and address potential vulnerabilities before they can be exploited.

This requires forward-thinking policies and adaptive security frameworks and long-term investments in technology. The U.S. government and private sector need to develop comprehensive strategies that not only address current security challenges but also anticipate future threats. These policies should be flexible enough to evolve with the rapidly changing technological landscape. Adaptive security frameworks should incorporate principles of resilience, allowing systems to detect, respond to, and recover from security incidents quickly.

Capital investments in cutting-edge security technologies and innovation hubs focused on cybersecurity research and development are crucial components of this approach. Additionally, streamlined procurement processes can ensure that organizations can quickly adopt and implement the latest security solutions. By fostering collaboration between the public and private sectors, as well as academia, we can create a robust ecosystem of innovation and security that is better equipped to face the challenges of technological acceleration.

5. Status Quo Business Processes

Supply chain attacks. Cyber threat actors' exploitation of critical vendors has highlighted the need for robust cyber supply chain risk management and vendor vetting. From the SolarWinds Orion platform breach in 2020 to Okta in 2023, the concentration of risk in and across supply chains demands constant attention. Third party risk management is a critical part of supply chain security, and I was encouraged to see that the National Institute of Standards and Technology (NIST) added cyber supply chain risk management across several publications in the last four years, including the Cybersecurity Framework 2.0.

Investments, Mergers & Acquisition. Cybersecurity challenges are commutative and can transfer during mergers and acquisitions. The United States' historical openness to foreign investment has also been exploited by competitors. The National Counterintelligence and Security Center (NCSC) has issued guidance warning start-ups that foreign threat actors could invest in their companies to "harm U.S. economic and national security interests." The FBI is reportedly investigating Hone Capital, which launched in 2015 with an initial investment of $115 million from a Chinese private equity group and has invested in over 350 U.S. tech startups. The investment has allegedly resulted in the transferring of trade secrets and intellectual property back to Beijing.

It is imperative to invest capital in technologies that adhere to U.S. law, conform to U.S. sanctions, and are not subject to the jurisdiction of adversarial nations before they go to markets. These trusted capital principles promote security, trust, safety, and national security *before* products go to market. When the company is secure by design and intent, the digital ecosystem it then joins is, too.

This complex and multi-actor threat demands of us sustaining investments in innovative, intrepid, and industry-led solutions.

B. Policy Recommendations

We must strengthen national cybersecurity by prioritizing security across all lines of efforts by clarifying roles and responsibilities of the private sector and government, upskilling our collective workforce, and embracing technological innovation that will enhance the resilience of our infrastructure against cyber attacks. These strategic investments will yield greater returns in our security.

1. Policy Solutions to Clarify Roles and Responsibilities

Continue Building Mechanisms to Measure Progress. Government efficiency depends on good data and clear-eyed analysis. We cannot understand what works without data. We need a repository of data in this area to know what cybersecurity regulations and programs to keep and what to cut.

Clarify Lawful Proactive Solutions for Industry and Improve the Cybersecurity and Information Sharing Act of 2015 5 U.S.C. §§1501-1510. The current state of U.S. infrastructure vulnerability is unacceptable. Power grids, transportation systems, water supplies, and communication networks are all in jeopardy. You can send a clear message: the United States will defend itself against cyber aggression with the same resolve as it defends against physical threats. Everything from defensive measures to offensive operations should be on the table. Crooks, spies and terrorists should be hunted jointly with key private sector actors. Efforts to "defend forward" must be continued in conjunction with providing resources and assistance to critical, often overlooked entities such as small businesses and rural communities. Further, we must leverage the U.S.'s unique combination of innovation and capital investment to support and incentivize in areas of the world aligned with U.S. interests.

Industry cannot defend the infrastructure the Nation relies upon without the assistance of the U.S. government and its allies. We cannot expect industry alone to defeat nation-state actors. The Cybersecurity Information Sharing Act of 2015 was a good start to encouraging better collaboration between the private sector and government. Congress authorized certain protections to industry if they shared cyber threat indicators and defensive measures within industry and with the government for cybersecurity purposes. As the law is up for renewal, Congress should consider more precision in defining defensive measures (5 U.S.C. §650) so that the lines between proactive defense and "hacking back" are clearer. Most importantly, this Committee must take action to reauthorize CISA 2015 before it lapses in September to ensure we do not see hard won progress lost to Congressional inaction.

Prioritize Cybersecurity Regulatory Alignment and Streamlining. Regulatory harmonization is another key issue for the Committee to consider. Under my leadership at ONCD - and in alignment with the National Cybersecurity Strategy Implementation Plan - we put out an extensive request for information to the private sector to understand their challenges with overlapping regulatory regimes. What we heard was startling. Businesses of all sizes and from 11 of the 16 critical infrastructure sectors reported that the compliance burden was hampering their cybersecurity programs. One industry group reported that CISOs were spending 30 to 50 percent of their time focused on compliance. This is not only a drain on our economy - it actually leaves us less secure, by keeping cyber operators filling out paperwork instead of defending systems.

Last Congress, Senator Peters, Senator Lankford, and Congressman Higgins introduced legislation to help bring coherence to the multitude of Federal regulatory approaches. The bill would have empowered the National Cyber Director to convene all of the relevant parties, including independent regulators, to develop a set of cross-sector minimum requirements that would have reciprocity baked in. A business that operates in multiple sectors - or that is in the supply chain of many regulated entities - would only need to show they met the baseline once. I am very confident this approach will both meaningfully improve our cybersecurity posture and reduce compliance costs, and I hope Congress will continue last year's momentum and move swiftly to enact this legislation. In this post-Chevron era, the incoming Administration's work with Congressional leadership will be critical.

Of course, cybersecurity is a global challenge, and the regulatory landscape is changing swiftly internationally as well. Late last year, dozens of multinational chief information security officers sent a letter to senior leaders from the Organization for Economic Co-operation and Development (OECD) countries urging them to add regulatory harmonization to the OECD's digital agenda. This builds on work former DHS Secretary Mayorkas did earlier in 2024, in partnership with the European Commission, to catalog overlapping incident reporting regimes. I urge this Committee to champion international regulatory harmonization work, including through venues like the OECD, to ensure a level playing field across the markets of our allies and partners - and to achieve our shared interest in protecting our critical infrastructure from adversary nations and cyber criminals.

Support and Instantiate the Cyber Safety Review Board (CSRB). The Cyber Safety Review Board has played a critical role in fostering transparency and accountability and driving improvements across federal agencies and critical infrastructure providers. This Committee should consider how to codify and strengthen the CSRB's role in providing a mechanism to learn lessons from past incidents and strengthen our nation's cyber defenses. Steps to strengthen the CSRB include making a full-time, independent, non-partisan board, with a full-time technical staff and administrative subpoena power. Independence will enhance the credibility of CSRB's investigations and advice.

2. Policy Solutions for Investing in a Skilled Workforce to combat cyber threats

Expand support for the Federal Cyber Scholarship-for-Service Program. 5 U.S.C § 7442 and the National Center of Academic Excellence program in Cybersecurity. The integration of emerging technologies into legacy systems, the maintenance of those systems, and the security of technology requires a well-skilled workforce in the private and public sectors. Over the last several years, Congress has proffered positive legislation to improve our workforce. As succinctly described in the National Cyber Workforce and Education Strategy, Federal programs in cyber workforce and education reinforced the importance of sustained Federal investments by establishing a foundation for cyber workforce and education program development to provide a pipeline of qualified cyber talent. These legislative efforts include the National Center of Academic Excellence program in Cybersecurity led by the National Security Agency (NSA); the CyberCorps®: Scholarship for Service (SFS) program, led by the National Science Foundation (NSF) in coordination with the Office of Personnel Management and the Department of Homeland Security; the Department of Defense Cyber Service Academy; the Cybersecurity Education and Training Assistance Program led by the Cybersecurity and Infrastructure Security Agency; and the National Initiative for Cybersecurity Education led by National Institute of Standards and Technology.

Congress has an opportunity now to improve and expand upon these programs. It was necessary to bolt on cybersecurity to existing programs in the past, but it is now time to ensure that these programs are impactful and remain sustainable. To remain sustainable, Congress should expand the current programs in connection with the cyber workforce to (1) expressly authorize and appropriate CISA to carry out the responsibilities of DHS where appropriate under existing law, (2) provide resources to increase the number of internships and apprenticeships available to qualifying students from high-schools, two-year community colleges, or four-year universities, and (3) provide incentives to federal and non-federal entities for jobs placement to soft targets like our water and energy systems.

3. Policy Solutions to Better Integrate Technological Solutions for Mitigating Cyber Risks

Eliminate "Tech-Debt" - Technical debt, resulting from legacy IT and unsupported technologies, creates risk to operations, cybersecurity, and resilience, and creates inefficiencies and wasteful spending. The U.S. government and critical infrastructure providers must focus on eliminating technical debt by identifying existing technical debt and then modernizing IT infrastructure, including moving to the cloud and deprecating legacy IT systems.

Build Cyber Resilience and Response Capabilities. The choice between defense and offense is not binary. A game-winning interception steals the advantage from the offense and puts the team on the scoreboard. That's an offensive defense, and a principle our cyber resilience must consider. Continued investments in automated recovery, real-time threat detection, and security operations center (SOC) modernization will further advance the ball here.

Strengthen Critical Infrastructure as part of our National Defense. We need to correct foundational weaknesses in our Nation's critical infrastructure and defense systems, focusing on (1) securing supply chains, (2) protecting sensitive data, and (3) ensuring resilience against unauthorized access and emerging vulnerabilities. A legislative agenda focused on implementing secure-by-design principles, upgrading supply chain standards, and fortifying critical digital and physical systems will fortify our critical infrastructure against nation-state threats.

Promote the Use of Artificial Intelligence (AI) to Transform Cyber Defense. We have already seen the benefit of AI to cyber defenders, including using AI to more quickly identify threats and new vulnerabilities, and scale cyber talent. The federal government should build on this success to accelerate the development and deployment of AI and explore ways to improve the cybersecurity of critical infrastructure and small and medium businesses using AI. The federal government can achieve this acceleration through (i) funding of public-private pilots on the use of AI to enhance cybersecurity in critical infrastructure sectors, (ii) funding for large-scale, labeled datasets to make progress on cyber defense research, and (iii) prioritizing research and development on human-AI interaction methods to assist with cyber analysis and incident response.

Advance Threat Detection and Intelligence. The need for advanced threat detection and intelligence capabilities to counter both known and emerging threats is certain. A combined congressional and administrative agenda could focus on integrating AI, advanced analytics, and threat intelligence to enhance situational awareness and preempt adversarial actions in cyberspace and the information domain. Constant vigilance—like a digital See Something, Say Something program—will enable the foresight needed to defend and defeat malicious cyber actors. Further, to enable identification of threat activity, CISA's capability to hunt for and identify threats across Federal Civilian Executive Branch agencies under 44 U.S.C. 3553(b)(7) must be strengthened. This includes developing the technical capability to gain timely access to required data from Federal Civilian Executive Branch (FCEB) agency endpoint detection and response (EDR) solutions and from FCEB agency security operation centers.

Enhance Identity and Access Security. Distinguishing between our digital presences is - knowing who's who, and that you are you - is of paramount importance for cyber security. Compromises of identity and authentication are a leading attack vector that our adversaries exploit year after year; weak identity infrastructure also provides adversaries with the quickest and easiest way to monetize stolen data, given that many of the identity solutions we use online are built around the premise that "knowing several things about you" means "someone is you." Solving this will require that America addresses the gap between the paper and plastic credentials - such as driver's licenses, birth certificates, and passports - that work in the physical world and the lack of any digital counterpart that can be used to prove who you are in the online world. This is an area where government must play a bigger role – in that government is the only authoritative issuer of identity. Likewise, knowledge-based systems for identity proofing are vulnerable, so too are our knowledge-based systems such as passwords for authenticating. We need to continue to drive the adoption of more modern, robust authentication solutions such as FIDO passkeys and security keys that can stop phishing attacks cold. Identity and access management (IAM) remains a pillar of zero-trust architectures – and encouraging both government and private sector organizations to accelerate their adoption of a unified identity security program can streamline efforts to prevent unauthorized access, phishing, and email-based attacks.

C. Conclusion

The global cyber threat landscape requires a coordinated, proactive approach combining legislative action, technological innovation, and operational collaboration. By addressing these challenges through the framework I've outlined, we can better protect our national security interests while fostering innovation and economic growth.