United States Senate
WASHINGTON, DC 20510

September 7, 2023

Acting Director Kemba Walden
Office of the National Cyber Director
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC 20500

Acting Director Walden,

We write to you at a moment of remarkable technological innovation in the field of Artificial Intelligence (AI). We are collectively evaluating both the immense promise and sobering risks of AI, including capabilities we did not expect to see and those we do not always fully understand. Given the Office of the National Cyber Director's unique perspective in implementing the National Cybersecurity Strategy, we seek to understand how we can prevent emerging generative AI capabilities from being used to carry out sophisticated cybersecurity attacks.

The federal government has successfully been conducting advanced research in the fields of cybersecurity and AI. The bipartisan CHIPS and Science Act made generational investments into both the domestic production of advanced semiconductors that will power the AI revolution and the scientific research that will secure American leadership on the global stage. Prior to that, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 established the National AI Initiative and directed the Office of Science and Technology Policy to coordinate activities across the federal government to advance the safe and responsible development of AI. The National Institute of Standards and Technology released the AI Risk Management Framework which provides comprehensive guidance for developing and deploying advanced AI systems safely. Finally, the recently released update to our National Cybersecurity Strategy outlines a whole-of-government approach to secure our critical infrastructure at home and disrupt would-be cyberattackers in their tracks.

Cybersecurity professionals have a long history of using tools and techniques supported by AI to prevent, and respond to, malicious cyber activity. AI can help organizations produce key data insights to support network traffic analysis and intrusion detection operations. Other use cases allow defenders to sift through unknown software to identify and remove malware or filter out phishing messages before they reach their intended targets. Protecting our nation's cyber infrastructure requires leveraging all tools at our disposal, including applying AI techniques to improve cybersecurity defenses in organizations of all sizes and technical capacity.

Advancements in generative AI have raised new cybersecurity opportunities for both defenders and attackers. Frontier models are pushing the limits of computational power at scale and have the ability to process, translate between, and generate both natural languages and coding languages. Companies are already offering services to help individuals write code quickly and efficiently without introducing common vulnerabilities. Our country will benefit enormously from broadening the technical skills across our workforce by making software development more accessible and secure. However, bad actors can also leverage generative AI technology to accelerate their attempts to undermine established cybersecurity protections. As a result, attackers could profit by stealing money, data, and intellectual property from everyday Americans and the small businesses that power our economy.

As Congress considers how to further promote AI innovation that is responsible, transparent, and advances our nation’s cybersecurity, we request your response to the following questions:

1. How can defenders of critical infrastructure leverage AI to secure their systems?
    a. Can generative AI help achieve the goals set out by the Cybersecurity and Infrastructure Security Administration’s Joint Guidance for manufacturers to produce software that is secure-by-design and -default?
    b. How can AI-enabled cybersecurity products and features make small businesses more resilient to cyberattacks?
2. Since the public release of accessible open source large language models, has there been any increase in cybercrime activity that can be attributed to fine-tuned AI models?
3. What recommendations do you have for private and public industries who may fall victim to adversarial AI-enabled Cyberattacks?
    a. How is ONCD tracking AI-enabled cyberattacks by foreign adversaries or non-state actors?
    b. Are there certain industries that are being targeted more than others?
    c. Is ONCD preparing any strategic plans for state and local governments to help prevent AI-enabled cyberattacks?
4. How does the new National Cybersecurity Strategy address risks posed by generative AI models?
    a. Are additions or changes needed to keep pace with this rapidly developing technology?
    b. How will the National Cyber Workforce and Education Strategy help build a cyber workforce capable of building and maintaining secure systems and what additional resources or policies will we need to achieve that goal?
5. What steps can developers take during the training, testing, and deployment phases of a product's lifecycle to prevent AI systems from facilitating attacks exploiting cybersecurity vulnerabilities?
6. Is the federal government developing partnerships with industry, academia, and

state/local governments to ensure coordination on resilient cybersecurity defenses in the era of generative AI?

We thank you for your attention to these issues and for your leadership advancing our national security and economic prosperity by securing our digital infrastructure.

Sincerely,

John Hickenlooper
John Hickenlooper
United States Senator

Thom Tillis
Thom Tillis
United States Senator