COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Subcommittee Hearing Statement of Ranking Member Bennie G. Thompson (D-MS)

Considering DHS' and CISA's Role in Securing Artificial Intelligence

December 12, 2023

This hearing builds on previous work in this subcommittee to understand how emerging technologies will impact our national security. In the last two Congresses, Chairman Richmond and Chairwoman Clarke held hearings on how AI, quantum computing, and other technologies would affect cybersecurity and how the Federal government can better prepare for their impact.

The release of ChatGPT last year demonstrated to the world what we already knew: that AI is not some hypothetical technology of the future, but a tool being used today with tremendous potential but also risks that need to be understood for effective security policymaking.

Fortunately, since taking office, President Biden has made developing AI policy a priority. The October release of Executive Order 14110 reflects months of consultations and is a comprehensive effort to ensure that agencies across the Federal government are working to address the full range of challenges AI presents, while harnessing its power to improve government services, enhance our security, and strengthen our economy.

I was particularly pleased to see that the EO incorporated the civil rights, civil liberties, and privacy emphasis included in the Administration's Blueprint for an AI Bill of Rights. AI systems are built by humans and therefore subject to the biases of their developers. To overcome this, addressing civil rights concerns must be baked into the AI development process, and I appreciate the Biden Administration's emphasis on this issue throughout the executive order. As we all know, good intentions are not enough, which is why Congressional oversight of the EO's implementation will be so important.

Today's hearing allows this subcommittee to hear the perspectives of leading AI industry stakeholders on how DHS and CISA can implement their responsibilities under the EO and how they can support the safe and secure use of AI.

For cybersecurity, AI offers tremendous opportunities to enhance the ability for network defenders to detect vulnerabilities and intrusions and respond to incidents. But, it also may be utilized by our adversaries to facilitate more attacks. And as generative AI continues to advance, the risk grows that deepfakes and other inauthentic synthetic content will be used to by foreign governments to undermine our democracy and by cyber criminals to facilitate their crimes.

DHS and CISA must have a central role in ensuring that AI technology improves our security rather than harms it. To do so, it will be essential that we consider perspectives of our private industry, where so much of the most advanced work in the world in AI development is taking place.I hope to hear more today on how DHS and CISA can best utilize AI, how they can support efforts to secure AI systems, and how they can reduce the risks AI may pose to critical infrastructure.

CISA's ongoing work on developing secure-by-design principles and its partnerships with critical infrastructure make it an essential part of the Administration's whole-of-government approach to AI policy and will allow CISA to build AI security efforts into their existing programs and policies. For CISA to carry out that role, it must have the proper workforce that understands AI and its security implications.

Building up our national talent pool of AI expertise and ensuring that Federal agencies can recruit and retain employees with the right skills will be essential if we are to address AI's challenges while utilizing its full potential. EO 14110 provides directives across the Federal government to strengthen our national AI policy, and I stand ready to partner with my colleagues on this committee to ensure DHS and CISA have the resources and authorities necessary to carry out their responsibilities.

# # #

Media contact: Adam Comis at 202-225-9978