COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

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

Advancing Innovation (AI): Harnessing Artificial Intelligence to Defend and Secure the Homeland

May 22, 2024

Artificial intelligence is not new. The Department of Homeland Security and its components have a long history of trying to understand how to most appropriately leverage the capacity AI provides.

The release of ChatGPT in November 2022 made clear AI's transformative potential, and it accelerated efforts by the Administration and Congress to ensure the United States continues to lead the world on the responsible development and use of AI. As we consider how to deploy AI to better secure the homeland, we must keep three critical principles in mind.

First, we must ensure that AI models we use and the data to train them do not reinforce existing biases. That requires that AI used by the government be developed pursuant to specific policies designed to eliminate bias and is tested and retested to ensure it is not having that effect. Eliminating bias from AI also requires a diverse AI workforce, comprised of people from a variety of backgrounds who can identify potential biases and prevent biases from being encoded into the models.

Second, the government must rigorously assess appropriate use cases for AI and ensure that the deployment of AI will not jeopardize the civil rights, civil liberties, or privacy of the public. Law enforcement and national security agencies, in particular, must implement an exacting review of potential infringements on these foundational democratic principles.

Moreover, it is essential that the workforce be included in decision-making processes on how AI will be deployed. The workforce is in the best position to understand capability gaps and where AI could add efficiencies. AI is a tool the workforce will use to carry out their jobs more effectively. It is not - and should not ever be - a replacement for people.

Finally, the AI tools we use must be secure. In many respects, existing cybersecurity principles can be adapted to secure AI. I commend the Cybersecurity and Infrastructure Security Agency (CISA) for working with the private sector to ensure the adoption of Secure-by-Design principles in the development of AI. Moving forward, we must determine vulnerabilities unique to AI and work together to address them. I commend President Biden on last year's Executive Order on AI, which put the Federal government on a path of developing and deploying AI in a manner consistent with these principles.

As DHS continues to assess how it will use AI to carry out its vast mission set – from cybersecurity to disaster response to aviation security – I am confident that it will do so in a manner that incorporates feedback from the workforce and protects civil rights, civil liberties, and privacy. We cannot allow our optimism about the benefits of AI to short circuit how we evaluate this new technology. At the end of the day, bad technology is bad for security.

As we consider the potential benefits AI presents for DHS's mission, we must also consider the new threats it poses. AI in the hands of our adversaries could jeopardize the security of Federal and critical infrastructure networks as well as the integrity of our elections. We know that China, Russia, and Iran have spent the past four years honing their ability to influence our elections, sow discord among the American public, and undermine confidence in our elections results. Advances in AI will only make their job easier, so we must redouble our efforts to identify manipulated content and empower the public to identify malicious foreign influence operations.

I look forward to a robust conversation about how the Department of Homeland Security can use AI strategically to carry out its mission more effectively.

# # #

Media contact: Adam Comis at 202-225-9978