COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

**FOR IMMEDIATE RELEASE**

# Hearing Statement of Cybersecurity & Infrastructure Protection Subcommittee Ranking Member Eric Swalwell (D-CA)

## *Security to Model: Securing Artificial Intelligence to Strengthen Cybersecurity*

**June 12, 2025**

Every day, we learn about a new evolution in artificial intelligence. Innovators across the world are developing new use cases for AI and building its capacity to take on more complex tasks more independently and more quickly. My district is home to many of the best minds in the business – the students, startups, and scientists racing to develop the next breakthrough.

I am lucky to have the opportunity to speak with them when I go home, and I'm glad Committee members had the opportunity to come to the West Coast to meet them last month. I want to highlight something the smartest people in my district tell me: We don't have to sacrifice security to innovate. Security and innovation can - and must - coexist.

I am concerned that we too often perceive security and innovation as inversely related – a zero-sum game – and it is not. For years, we have attributed poor security in the technology we use everyday to the "race to market." But the evangelization of Secure by Design guidance and improvements in technology enable tech developers to integrate security into their products from the start, reducing the friction and delays associated with building in security at the end of development. Tech developers can get their products to market both quickly and securely.

Right now, the United States is competing to maintain global dominance in AI. There is pressure to develop and deploy quickly and for the government to remove barriers to AI innovation. Like the Biden Administration, the current Administration is encouraging departments and agencies to accelerate the deployment of AI on Federal networks. I am committed to supporting efforts to keep the United States the global leader in AI, and I am excited about the potential of AI to make government services more accessible and more efficient for the public. And fortunately, none of this requires us to sideline security. It demands that we embrace it.

Today, we will hear from witnesses who are experts in securing AI. They will help us understand what the Federal government and other end users should be asking of AI vendors, the roles and responsibilities for security, and how to monitor and maintain the security of AI once it is deployed to make sure it's performing as intended. Although members of the Administration have made comments suggesting that security is a barrier to innovation, I am pleased that the Administration's policies – namely the early April OMB memos – maintain the commitment to security adopted by the Biden Administration.

Moving forward, I look forward to working with the Administration to ensure that the Federal government is providing the right guidance – from agencies like CISA and NIST – to promote the development and deployment of secure AI. AI without governance is a recipe for disaster. Additionally, I will be interested in understanding how we can leverage and augment existing security program – like CDM – to ensure the security of AI once it is deployed on Federal networks.

And, finally, I am interested in understanding challenges in procurement that frustrate the Federal government's ability to use cutting-edge technology quickly. I would be remiss if I did not express my concern about the brain drain at Federal departments and agencies responsible for supporting efforts to develop, deploy, and secure AI. There has been an exodus of talent from CISA, NIST, NSF, and every procurement and CIO shop across the Federal government. The Federal government will not be able to harness the full potential of AI if we don't have a workforce who understands how to procure it and secure it.

# # #

Media contact