COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

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

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

December 12, 2023

The potential of Artificial Intelligence has captivated scientists and mathematicians since the late 1950's. Public interest has grown each time AI has achieved a new milestone - from Watson beating Ken Jennings at Jeopardy to AlphaGo defeating the World Champion Go player in 2015 to the debut of ChatGPT just over one year ago today.

The developments in AI over the past five years have generated interest and investment and served as a catalyst to drive public policy that will ensure that the United States remains a global leader in innovation and that AI technology is deployed safely, securely, and responsibly.

Over the past year alone, the Biden Administration has issued a Blueprint for an AI Bill of Rights, a National AI Research Resource Roadmap, a National AI R&D Strategic Plan, and secured voluntary commitments by the nation's top AI companies to develop AI technology safely and securely. And just over one month ago, the President signed a comprehensive Executive Order that brings the full resources of the Federal government to bear to ensure the United States can fully harness the potential of AI while mitigating the full range of risks it brings.

I was pleased that the Executive Order directs close collaboration with our allies as we develop policies for the development and use of AI. For its part, CISA is working with its international partners to harmonize guidance for the safe and secure development of AI. Two weeks ago, CISA and the UK's National Cyber Security Centre issued *Joint Guidelines for Secure AI System Development*. These Guidelines were also signed by the FBI and NSA, as well as international cybersecurity organizations from Australia, Canada, France, Germany, and Japan, among others.

Moving forward, harmonizing AI policies with our partners abroad and across the Federal enterprise will be critical to promoting the secure development of AI without stifling innovation or unnecessarily slowing deployment. As we promote advancements in AI, we must remain cognizant that it is a potent dual-use technology.

Today, deepfakes are easier and less expensive to produce and the quality is better. That means that it takes relatively little skill for a jealous ex-boyfriend to produce a revenge porn video to harass and humiliate a woman, or for a criminal to produce a child abuse video. Deepfakes can also make it easier for our adversaries to masquerade as public figures and either spread misinformation or undermine their credibility. We must prioritize investing in technologies that will empower the public to identify deepfakes. Watermarking is a good start, but it is not enough.

The novelty of AI's new capabilities has also raised questions about how to secure it. Fortunately, many existing security principles - which have already been socialized – apply to AI. To that end, I was pleased that CISA's recently released AI Roadmap didn't seek to re-invent the wheel where it wasn't necessary,

and instead integrates AI into existing efforts like “secure-by-design” and “software bill of materials.” In addition to promoting the secure development of AI, I will be interested in learning how CISA can use artificial intelligence to better execute its broad mission set.

Already, CISA is using AI-enabled endpoint detection tools to improve Federal network security, and the Executive Order directs the Department to conduct a pilot program that would deploy AI tools to autonomously identify and remediate vulnerabilities on Federal networks. AI also has the potential to improve CISA’s ability to carry out other aspects of its mission, including its analytic capacity.

CISA’s success rests on its ability to analyze disparate data streams and draw conclusions that enable network defenders to protect against cyber threats and help critical infrastructure owners and operators build resilience by understanding critical risks and interdependencies. The enormity of this task continues to grow.

For example, Congress dramatically improved CISA’s visibility into malicious cyber activity on domestic networks by authorizing mandatory cyber incident reporting and the CyberSentry program – both of which will generate large amounts of new data that CISA must ingest, analyze, and action. Improved operational collaboration programs – like the Joint Cyber Defense Collaborative – will similarly yield more data that should inform CISA’s security products. I am interested in understanding how CISA can better leverage AI to scale and improve the analytic capacity that is central to its mission.

As a final matter, as policymakers, we need to acknowledge that CISA will require the necessary resources and personnel to fully realize the potential of AI while mitigating the threat it poses to national security. I once again urge my colleagues to reject proposals to slash CISA’s budget in FY24.

# # #

Media contact: Adam Comis at 202-225-9978