To: Interested Parties

From: Jason Green-Lowe, Executive Director - Center for AI Policy

Date: April 30, 2024

RE: US Senate Gets Ready to Pile More AI Responsibilities on NIST

_____

After months of debate, the US Senate has rolled out two new documents that could steer the future of AI safety:

1) Senators Mitt Romney (R-UT), Jack Reed (D-RI), Jerry Moran (R-KS), and Angus King (I-ME) unveiled the first congressional framework to deal exclusively with the extreme risks posed by future developments in advanced AI models
.
2) The "Future of AI Innovation Act," introduced by US Senators Maria Cantwell (D-WA), Todd Young (R-IN), Marsha Blackburn (R-TN), and John Hickenlooper (D-CO), provides staff and funding for voluntary evaluation of the safety of AI models and international coordination on best practices in AI risk management.

With major Senate committees likely to begin marking up legislation related to artificial intelligence soon, it makes sense that elected officials want to start shaping the debate. Based on discussions on Capitol Hill and CAIP's analysis, Senators want to ensure the United States remains at the forefront of global innovation while addressing the many concerns around AI's social impact and catastrophic risks.

The proposed measures are not blanket regulations for all AI – instead, they are narrowly tailored for only the most advanced models that are likely to pose the most extreme risks. The framework suggests implementing safeguards and oversight mechanisms for these high-risk AI systems to prevent their exploitation by foreign adversaries and bad actors.

The Romney framework calls out the risk that advanced AI could assist with the development of biological, chemical, cyber, or nuclear weapons. Section 102(c)(7) of the Cantwell legislation calls for testing and evaluation with respect to all of these risks, as well as potential threats to essential infrastructure and America's energy security.

These moves in the US Senate are not surprising - their constituents are calling for AI oversight. Research released by S&P Global Market Intelligence revealed that while consumers acknowledged the practical

applications of advanced AI tools, they also harbored significant worries about AI's capacity to displace jobs, enable fraud, be misused, and even develop sentience. According to an April 2024 survey by SEO expert Mark Webster, [79% of Americans want strict AI regulation](#).

These two Senate documents are a big step forward for AI safety – both sets of Senators are thinking carefully about what new software features will be needed to keep Americans safe as AI technology advances and how we can incentivize companies to develop those features. The Cantwell legislation also calls upon the Department of Commerce, the State Department, and the White House Office of Science and Technology Policy to forge international alliances to achieve consensus with like-minded governments on AI standards. The Center for AI Policy (CAIP) is thrilled to see these documents enter the public discussion.

That said, neither the Romney framework nor the Cantwell legislation is likely to fully satisfy the public's demand for effective regulation, because they aren't set up to create a dedicated AI regulator. Instead, Sen. Cantwell's legislation would create an "AI Safety Institute" within NIST, the National Institute of Standards and Technology. Similarly, the Romney framework is agnostic about whether a new regulator is needed, suggesting that "Commerce could leverage the National Institute for Standards and Technology (NIST) and the Bureau of Industry and Security to carry out these responsibilities."

Dumping the responsibility for AI safety onto NIST is counterproductive, because NIST is committed to working with *voluntary* standards – they're not interested in taking on a regulatory role. As NIST's chief AI adviser [Elham Tabassi](#) put it, "Our job is to help industry develop technically sound, scientifically valid standards. We are a non-regulatory agency, neutral and objective." NIST derives much of its moral authority and technical insights from the fact that industry is willing to cooperate with it because labs trust that the information they share won't be used against them.

Setting NIST up as an enforcer undermines that trust. Instead of piling more responsibilities on NIST's busy shoulders, Congress should be looking to create a dedicated office that can handle the important work of AI safety enforcement.

These recent moves by US Senators underscore a crucial period of technological transformation and opportunity in AI governance. CAIP will play a role in this period and is keen to work with Senators to advance principles and policies that mitigate the catastrophic risks of AI.