STATE OF MICHIGAN
JOCELYN BENSON, SECRETARY OF STATE
DEPARTMENT OF STATE
LANSING

AI Insight Forum: Elections
November 8, 2023

Written Statement from
Michigan Secretary of State Jocelyn Benson

Thank you, Leader Schumer, the AI Caucus and the Senators and Staff hosting today's important conversation.

I am grateful for the opportunity to appear today on behalf of the voters of Michigan and as a representative of the larger community of state election officials charged with administering free and fair elections across our country.

As Michigan's Secretary of State, I serve as the state's chief election officer. My responsibilities include ensuring elections in every one of our 83 counties and 1,520 jurisdictions are secure and accessible. On both fronts we are thriving. Michigan's 2020 and 2022 elections shattered previous voter turnout records and in 2022 we led the nation in turnout among young voters. Our decentralized system ensures layers of security protocols exist at every level, affirmed through continual statewide and local post-election audits that consistently confirm the security and accuracy of our procedures.

As the chief elections officer of a battleground state, I am acutely aware that the biggest threat to election security today is misinformation and disinformation designed to confuse voters and obfuscate the voting process. Artificial Intelligence will amplify and expand exponentially these tactics and their impact.

That's why our topic today is both timely and necessary.

Long-term, Artificial Intelligence may help democratize our elections in ways that expand access and enhance our security.

But recent advances in AI create uncertainties as we approach the forthcoming consequential presidential contest in 2024.

We should expect bad actors, both foreign and domestic, to use AI to *divide*, *deceive*, and *demobilize* voters throughout our country over the next year.

Federal and state officials have a responsibility to strengthen election security and combat election interference. While prior sessions of this Forum have touched on

general challenges arising from deepfakes, candidate impersonation, and questions surrounding campaign advertising, I will focus my statement on **five challenges** that I believe are particularly acute for election administrators.

First, AI makes it **easier to create and distribute hyperlocal disinformation** that misleads voters about the voting process or conditions at their polling site. Bad actors may misuse public data about voting locations to produce highly specific claims about long lines or even violence to suppress the vote in key precincts. While voter suppression is not new, **AI tools supercharge the ability to generate large volumes of believable-sounding claims and to distribute those messages at scale.**

For example, one voter might get a text warning of long lines at his particular precinct, while another might see a social media post claiming her polling location moved because of flooding. The ability for AI to create content that includes specific details–like the name of individual voting sites–makes it more likely that voters will be misled.

Current federal law criminalizes certain types of interference in the exercise of our civil rights–including voting–and the Senate should consider whether using AI in the commission of those crimes should be made an aggravating factor or sentencing enhancement.

Additionally, while social media and messaging platforms are not liable for content posted by third parties, **the Senate should ensure tech companies are under no illusion: Section 230 does not shield big tech from liability when their own AI models produce harmful content**.

Second, I am concerned **AI tools could specifically target language-minority voters in uniquely harmful ways**. Foreign influence operations once required significant resources to produce credible-sounding claims in different languages. But Large Language Models (LLM) and Massively Multilingual Speech (MMS) models make it easier to adapt disinformation and propaganda to reach more communities.

Misinformation may be translated seamlessly across numerous languages, likely flying under the radar of fact-checking organizations. Critically, bad actors largely rely on social media and messaging services to distribute misinformation. That means **platforms like TikTok, Facebook, YouTube, Twitter, WhatsApp, and others have an opportunity to prove their commitment to election integrity by taking action to protect language-minority communities on their platforms.**

This Forum and individual Senators should continue pushing Big Tech companies to be transparent about their efforts to protect users, including non-English speakers. **The Senate should settle for nothing less than unequivocal commitments that these platforms' integrity tools are equally effective across languages.**

Additionally, closed messaging services like WhatsApp remain incredibly popular among many language-minority communities, and that app now allows for messaging to

hundreds of users simultaneously. Senators should press Meta to explain why its voter suppression policies do not extend to WhatsApp.

Third, **AI could greatly increase harassment and threats directed at local elections administrators and volunteers.** Those seeking to discredit and intimidate elections officials may use AI to "flood the zone" with large volumes of inflammatory and threatening content that creates confusion among voters or even incites violence. Local officials and poll workers lack the resources to protect themselves and their families—this must not be the price of public service. We know intimidation is pushing good people out of these positions and we cannot allow AI to make things worse.

Local volunteers and officials don't ask for the spotlight, but they deserve our protection. The **Senate should consider how to enact greater protections to deter doxing, intimidation, and mass harassment of those who administer the voting process.**

Fourth, **we must defend against the inequitable use of AI in voter purges**. The National Voter Registration Act requires states to establish a program of uniform list maintenance. But over-eager jurisdictions, politically motivated state legislatures, or outside groups may use AI-enabled systems to push the boundaries of that federal requirement. For example, AI models trained on prior list maintenance data may perpetuate systemic biases that disparately impact communities of color, college students, people experiencing housing insecurity, and other targeted populations.

Especially in an election year, fights over the use of AI in list maintenance and voter challenges should not be left to the courts. Congress is best situated to **clarify how AI can–and importantly cannot–be used to purge voter rolls** and I urge you to consider legislation that does so.

Finally, AI underscores the need for a **renewed federal investment to harden state elections systems against cyber attacks**. AI introduces a level of "speed, scale, and sophistication" that is difficult for under-resourced state agencies to counter alone. New AI systems are increasingly used to exploit vulnerabilities in code, to supercharge phishing, and to introduce ransomware that could cause a catastrophic systems freeze in an unprepared state.

Adversaries who target our states have nation-level resources, and our states should have nation-level resources committed to the defense of systems critical to our democracy. I urge you to consider ways to support and bolster state cybersecurity infrastructure in this evolving threat environment.

Thank you for the opportunity to submit this written statement, and for hosting this critically vital conversation. I look forward to our discussion and related follow up actions. Time is of the essence.