NATIONAL ASSOCIATION of
STATE ELECTION DIRECTORS

Thank you Majority Leader Schumer and Senators Rounds, Heinrich, and Young. I appreciate being asked to participate in this important conversation to represent the National Association of State Election Directors (NASED).

My name is Amy Cohen; I am the Executive Director of NASED, a nonpartisan, nonprofit membership association for the state and territorial officials whose primary responsibility is the administration of elections. Our members are in all 50 states, the District of Columbia, and the five US territories. In the 40 states where a Secretary of State or Lieutenant Governor is the Chief Election Official, NASED's member works for the Chief Election Official[1]; in the other 10 states, District of Columbia, and the five territories, NASED's member is the Chief Election Official.

No NASED members are elected[2]. Our members are public servants who oversee the implementation of election systems, laws, and policies, and work with local election officials. NASED does not issue best practices or guidance – we facilitate information sharing across the states and territories and from the federal government to the states and territories. NASED does not take positions on federal or state legislation or on federal or state election policy.

Based on a number of conversations I have participated in about Artificial Intelligence (AI) in elections and democracy, there is a tendency to conflate or combine campaigns and elections. For election officials, these are distinct. Campaigns are about policy, where candidates stand on the issues, and who wins; elections are about making sure voters can participate in the process, cast their ballots, and have confidence in the outcome. NASED's interest is only in the latter. To be clear, from our perspective, advertising falls in the campaign bucket.

When speaking strictly about election administration, much of the discussion about AI centers on false information. Generative AI technologies make it easier and less expensive to create inaccurate information about the administration of elections. The existing media ecosystem allows all information – accurate or not – to spread and to do so quickly, thus making AI a cheap and easy tool for actors looking to create and spread false information. But inaccurate information about the administration of elections also dates back to the earliest American elections, so it is important to think about the risks of AI to our field in that context. Election officials have confronted things like "Democrats vote on Tuesday, Republicans vote on Wednesday" or "vote by phone" for as long as our profession has existed. It moves significantly faster now, and the internet means that nothing stays local, but the concept of false information in elections and the challenge for election officials of responding to it is not new.

[1] In Kentucky, NASED is represented by the State Board of Elections, which is an independent agency from the Secretary of State. The Executive Director of the State Board of Elections does not report to the Secretary of State, although the Secretary is the Chief Election Official.
[2] In one state, the Secretary of the Senate, by statute, also serves concurrently as the Secretary of the State Board of Elections. The Secretary of the Senate is elected by the State Senate.

Despite this measured perspective, NASED's members are concerned about AI's ability to cheaply and easily generate deepfakes, or manipulated photos, video, and audio. Few people know the name of their State Chief Election Official, let alone what they look like or sound like; fewer still likely know the name of their local election official or what their local election official looks like or sounds like. A manipulated video of a Chief Election Official or local election official conveying inaccurate information about the processes or technologies in use in the election, or about how or where to cast a ballot, could be damaging and difficult to combat. Fortunately, most common AI image and video generation tools still have a tell, but as the technology improves, it will get harder and harder to identify images or video created by AI and it will require more and more time – our most scarce resource – for election officials to respond.

Unfortunately, it is my understanding that audio deepfakes are already there. There is no tell in audio – a voter cannot count fingers or look at the background – and audio-generated false information is already typically among the most difficult for election officials to address. Every election, voters receive robocalls with inaccurate information about participating in the election. The voters who receive those calls and recognize them as false information are not typically positioned to record the audio. Chasing down these reports is time consuming and labor intensive every single time. Now imagine if those robocalls imitated the voice of the State's Chief Election Official.

The election community has made a concerted effort over the last four years to direct voters to accurate and reliable sources of information about elections: their election officials. Our colleagues at the National Association of Secretaries of State developed the #TrustedInfo campaign in January 2020, and it continues to resonate. But AI generated audio, in particular, makes the effort to direct voters to the most accurate source of information more complicated: if the voice of your election official is saying it, and that person is the trusted source, should you believe it?

Finally, while many of our concerns focus on false information, it is important to note that AI lowers the barrier to entry for malicious cyber actors. The hallmark of phishing emails has long been that there was something "not quite right" about the language, often because they are written in English by non-English speakers. AI tools have made it easier for phishing campaigns to be effective across all sectors because it is now possible to create convincing phishing emails at little or no cost using AI. The same tools could also be used to generate malware and attach it to those phishing emails, compounding the impact of the original phish. For lower sophistication actors, this is a free upgrade, even if they have to do some work to make the malware more effective. Election offices are particularly cautious about phishing because they must open the emails they receive – voters and others send important documentation via email with attachments. While there are key cybersecurity mitigations in place in election offices to address the risks from unsolicited emails, the fact remains that humans are susceptible to phishing, and increased sophistication of phishing emails makes our community more open to risk.

As AI chatbots and tools proliferate, we would encourage the private sector companies behind them to consider the elections use-case from the beginning. These companies should build policies into their Terms of Use that limit how their technology could be used to create false information about elections. However, we would also encourage them to think about the reverse: how can their tools help educate people about election administration? From the election official perspective, the answer is easy. Actively promote election official websites and resources as the answers to all questions about elections. Do not rely on third parties to get it right and do not try to reinvent the wheel yourselves. It is not sufficient to decline to provide information. These applications should point people to the most reliable, accurate sources of information about election administration: election officials.

The private sector companies with publicly available AI tools have an opportunity to learn from the policy successes and failures of the social media companies. False information about elections does not stop and start on a predictable schedule. Three full years later, and every election official I know talks about the 2020 election every single day, answering questions from voters, the press, legislators, and courts about the conduct of that election. Many are still dealing with threats and harassment stemming from the 2020 election. Thus, publicly available AI tools must continuously promote election officials as the best source for information about election administration. This is not something that should be turned on and off depending on where we are in the calendar. “Election season” is 365 days a year, every year.

Over the last several months, digital watermarking has entered the conversation as a solution to help validate AI generated images and documents. While I cannot comment on the technical feasibility of the solution itself, I would note that without a human readable component, this would likely do little to affect how AI generated content with false information about elections spreads. If it requires technical expertise or advanced knowledge to verify an image, most will not do it, especially on a topic like elections where emotions, not logic, tend to govern behavior. To this day, misinformed people continue to spread widely debunked false information, including images and video, about previous elections. To be effective for our field, watermarking needs to be handled consistently across the internet and must be human readable.

Based on my conversations with election officials nationwide, all anticipate that AI technology will exacerbate existing risks within our field, from false information to phishing to malware. It is not clear to us at this time if AI creates any new risks to elections. While it is unlikely any policy solution will, at this point, have an impact on the 2024 presidential election, we agree that the impacts to election administration should be part of the discussion about the future of AI.