Cybersecurity: Artificial Intelligence

The 60-Second Security Series is intended to help election officials quickly identify, and address, potential security issues. Each topic includes a brief description, a list of security measures, and potential funding sources for making these improvements. More information about election security can be found at www.eac.gov.

Artificial Intelligence (AI) and Election Administration

Artificial Intelligence (AI) powered tools have become much more widely available and capable in recent years. AI tools have the potential to benefit society and election offices but can also accelerate false or biased information and undermine fair elections if used inappropriately. While these tools do not necessarily introduce new cybersecurity risks, AI tools may allow existing threats to scale more quickly and effectively. AI-generated text can dramatically increase the success rate of phishing emails and other social engineering attacks. According to the Cybersecurity and Infrastructure Security Agency (CISA), these types of attacks can deceive victims into providing their login credentials or installing malicious software. State and local election officials should also be aware that text, images, video, and audio content may be used to imitate themselves or other official sources of information.

Additionally, AI is becoming more prevalent within applications used by voters to find information, whether they are aware or not, either through AI-enhanced search or productivity tools. AI-generated information may seem plausible, but it is often inaccurate. This lack of accuracy may be particularly harmful to voters. Critical voting information, such as voting dates, hours, and locations, require a higher degree of accuracy than many AI tools can currently provide.

Definition:
Large Language Model (LLM)

Chatbots like ChatGPT are Large Language Models (LLMs), a type of generative AI that learns to recognize and mimic human speech by analyzing vast quantities of text. These tools are advanced enough to provide plausible responses to many prompts, but the answers generated are not always correct. Both the data used to "train" these models and user feedback over time can affect the quality of the response, but why an LLM provides any particular response is often unclear.

The purpose of this document is to provide practical and useful resources to election officials to counter information security and cybersecurity threats related to AI in the context of election administration.

Security Measures

There are several important steps that you can take to improve your office's security that relate to the possible threats posed by AI tools:

Information Security

Election officials will likely face information security threats based on inaccurate or low-quality information about election administration. The sources of this information could be generated directly by an AI chatbot, or AI tools could be manipulated to produce inaccurate or inauthentic information. Here are some tips to counter information security threats:

○ **Physical Materials**

Create written materials that point to your office's official sources of information, including websites and social media feeds. These can be palm cards distributed at your office, bookmarks at your local library, direct mailings to registered voters, or other printed materials likely to be seen by your constituents. A handout template can be found in the EAC's AI Toolkit for Election Officials.

○ **Social Media**

Establish your office as a clear source of information by posting consistently on social media. While there are a variety of platforms, only use networks that work for your office, keeping in mind the staff time and resources required to build an audience. Social media posts are best when kept clear and concise, especially if they are about complicated topics like voting by mail or curing a signature. Some offices use social media post schedulers to ensure their offices publish posts at least a few times each week. The EAC provides several toolkits and resources to help election officials effectively communicate with voters.

Cybersecurity

In addition to information-based threats, AI tools also pose more traditional cybersecurity threats to elections offices. Some of these threats are outlined below.

○ **Impersonation via Inauthentic Images, Video, or Audio**

AI tools can quickly and easily impersonate virtually anyone with only a small sample of that individual's image or voice. These tools may take advantage of the public nature of election administration to impersonate an election official. To limit the reach of this inauthentic information, be prepared to point local media and the public to your official communication channels, including verified social media accounts or government websites. Governments at all levels are eligible to host their materials on a .gov domain, which clearly identifies a website as coming from an official source. Additionally, election officials can find resources to restrict the amount of their personal data online on the EAC's website, including removing their personal information from Google search results.

○ **Advanced Phishing Emails**

In the past, phishing emails were relatively easy to spot due to incorrect (or even strange) wording or grammar. AI chatbots can be used to correct these issues while also creating plausible text that may elicit a response. Due to the increased complexity of phishing emails, it is important to be cautious when clicking any links or attachments. Look closely at the email address of the sender, ensuring that both the name and email address are from known people. Consider the context of the email. Was this an attachment you were expecting, or did it come out of the blue? If something looks suspicious but appears to be coming from a known sender, try calling the individual to confirm that the email is authentic.

○ **Cybersecurity Best Practices**

While the type of threats posed by AI tools is not new, this technology can dramatically increase the volume and sophistication of cyberattacks. Ensure that your office's cybersecurity practices are up to date. Keep backup records of critical information on separate systems or on paper. Use multi-factor authentication for all essential systems. And be sure to follow your office's guidelines for updating and maintaining your devices. Additional resources can be found in the Cybersecurity and Infrastructure Security Agency's (CISA) latest guidance on Generative AI and the 2024 Election Cycle and Cybersecurity Toolkit and Resources to Protect Elections.

Funding Opportunities

HAVA Election Security Funding

On February 14, 2024, the EAC unanimously voted to allow HAVA Election Security grant funds to be used to counter AI-generated threats to election administration. These funds may be used to fund voter education efforts, including the communication of official information about the voting process. Additionally, the EAC has published further guidance related to the use of HAVA funds to counter AI-generated mis- and disinformation. States can reach out to the EAC's OGM via email to clarify any concerns about allowability and allocability for specific activities and costs. For more information and to review the latest guidance on allowable uses of HAVA funds, go to the EAC Office of Grants Management or EAC Grants Guidance, or email grants@eac.gov.