Artificial Intelligence in Elections

Generative Artificial Intelligence (AI) is a technology that can create images, text, and videos with very little instruction from a user by learning patterns from very large datasets to predict the most likely response to a given prompt. For instance, text driven AI is trained on very large volumes of text, like blog posts, books, social media sites, and the like to learn how words and phrases are most likely to fit together. Similar approaches are used to "teach" AI how images should looked based on a text description, how a objects might relate to each other to look like natural movement. These technologies are advancing at a rapid pace, presenting opportunities and risks for individuals and society.

Like most tools and technologies, generative AI can be employed to improve and to harm election administration. "Deepfakes" are videos with recognizable people, such as an election official, but the actions and words of the people are created using generative AI. The same holds true for generating inaccurate news articles and social media content. OpenAI's ChatGPT and Google's Bard are generative AI platforms that create text based on a user's prompt. Another type of generative AI platform uses a text prompt to create images. Examples of this type of generative AI platform include Midjourney and DALL-E.

Generative AI platforms pose a risk to elections due to their ability to quickly generate inaccurate information and other misleading materials. While there are benefits of generative AI, election officials need to be aware of the risks that generative AI poses on elections and implement safeguards to prepare for the 2024 presidential election year.

Dissemination of misinformation is generative AI's most apparent risk to elections. This technology can create inaccurate content that bad actors can then spread through other forms of media. Election officials have a lot to juggle on election day and the days leading up to an election. However, generative AI capabilities have the potential to make the job of election officials more difficult. Here are a few examples to explain how this can happen:

- Election officials work diligently to communicate information such as election deadlines, polling locations, and voting hours. With generative AI, media such as news articles, social media content, etc., can more quickly be generated and used to deceive voters and provide them with inaccurate information.
- Generative AI can create images and videos using a simple prompt. Generative AI platforms can be used to attack an election official's integrity by misrepresenting or fabricating a statement or act of an election official.
- Phishing emails are already a known cybersecurity threat. Generative AI can create convincing phishing emails that are nearly indistinguishable from a reputable email, elevating this threat.

As technology advances, generative AI platforms are becoming more intelligent. Therefore, it is important for election officials to be aware of new advances in generative AI so that they can take appropriate measures to mitigate it.

Goals

1. Know the definition of Generative AI (Level 1 maturity)
2. Understand the potential impact of Generative AI on election administration (Level 1 maturity)
3. Understand how to manage the additional risks presented by Generative AI (Level 1 maturity)

Actions

For Artificial Intelligence in Elections, the necessary actions are the same for all maturity levels.

Generative AI is a rapidly evolving technology in today's society, and, unfortunately, we cannot control it or avoid it. However, we can take measures to mitigate the potential effects of generative AI on elections. Here are a few recommendations:

1. Establish your office as a trusted source. Ensure the public knows where to go for accurate election information. Use your organization's website, social media platforms, local media, and press releases to accomplish this.
2. Monitor social media for potential misinformation. Prebunk, debunk, and report misinformation as your office sees fit.
3. Practice good cyber hygiene by implementing the best practices in this guide that align with your maturity level. Use strong passwords and multi-factor authentication. Also, include guidelines on generative AI platforms in your organization's cybersecurity policies.
4. Provide training. Generative AI technology is becoming more advanced each day. To stay educated, provide cybersecurity training to staff members including AI awareness and phishing campaign assessments. This reduces the risk of falling victim to AI.
5. Use available resources. Take advantage of CISA's Cybersecurity Toolkit to Protect Elections.

Cost-Effective Tools

- CISA's Cybersecurity Toolkit to Protect Elections.

Mapping to CIS Controls and Safeguards

- CIS Controls associated with this best practices are addressed in the referenced actions

Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices