BRENNAN CENTER FOR JUSTICE | The Elections Group

Read the complete AI scenario planner here.

CHECKLIST

How Election Officials Can Mitigate AI Threats to the 2024 Election

MAY 2024

It will be challenging to implement all the measures needed to mitigate artificial intelligence threats before the 2024 general election. This checklist highlights actions that are most achievable ahead of November. Further details on these actions are outlined in our AI scenario planner.

I. Understand What AI Can Do

- Read the "Understand What AI Can Do" section.
- Familiarize yourself with and test AI content generation and deepfake detection tools with your communications, legal, IT, and operations teams.

II. Take Control of Your Online Presence

- Use a .gov website.
- Register, verify, and secure accounts on all major social media platforms. Make sure to:
  - Enable multifactor authentication and include a link to your official .gov website on all social accounts.
  - Conduct security checkups for all official and personal social accounts.
  - Conduct regular impersonation checks across social media and the internet, using Google searches and alerts.
- Develop a public service campaign to inform your community that:
  - Bad actors may try to mislead them about elections.
  - You are the source of official, reliable election information (make sure to share all your contact information). ** Pro Tip: HAVA funds can be used for this voter education campaign.

III. Prepare for Rapid-Response Communications

- Prepare a proactive campaign to get ahead of potential bad information.

- Develop and practice a crisis communications plan with holding statements for potential scenarios. Identify internal and external communicators who you can rely on if needed.
- Engage local media, community leaders, other government agencies, and campaigns to ensure they know who you are, how to contact you, and what your official social media accounts and websites are.

IV. Adopt Cyber and Physical Security Best Practices

- Enable multifactor authentication on all accounts, and leverage password managers to keep passwords secure for website administration tools, social media accounts, email and administrator tools, and phone and internet service providers.
- Use secure authentication practices when communicating with "trusted" people. i.e., establish code words, other knowledge-based protocols, or secondary out-of-band authentication before sharing sensitive information with teammates over the phone or online.
- Ensure operating systems and software on devices connected to the internet are updated to the latest versions.
- Ensure technical support is available during the election period.
- Use the Cybersecurity and Infrastructure Security Agency's (CISA) recommended security services, including:
  - automated vulnerability scanning
  - physical security and cybersecurity assessments
- Ensure staff complete the phishing and ransomware training that CISA offers.
- Encourage staff to use services such as DeleteMe to remove personal information from online data brokers and make social media accounts private.

V. Build and Strengthen Relationships with Technical Service Partners

- Learn how to notify social platforms of content on the electoral process, such as misleading information about when, where, and how to vote, that violates their terms of service.
- Establish a direct line of communication with your hosting provider so you can engage them in case of a security incident.

VI. Create Escalation Plans

- Include AI-based threat scenarios in your new or existing continuity-of-operation or incident-response plans to ensure speedy escalation and reduce remediation time.
- Ensure you have contact information for local, state, and national support organizations.
- Practice implementing your escalation plan.

VII. Prepare Legal Support Network

- Meet with your local attorney to ensure they understand AI threats and are prepared to exercise available legal remedies. Ensure they are available before, during, and after the election.