Bipartisan Policy Center

October 2024

Preparing for Artificial Intelligence and Other Challenges to Election Administration

RESULTS FROM TABLETOP EXERCISES IN FIVE STATES DURING THE 2024 ELECTION

By Dean Jackson, Matthew Weil, and William T. Adler

Table of Contents

Key Findings

- Rapid advances in artificial intelligence (AI) have led to fears about novel threats to election administration. These fears have arisen during an already difficult time for election workers, who are facing incredible scrutiny, rising harassment, and serious safety threats—all stemming from the heightened politicization of their work.
- The Bipartisan Policy Center held five tabletop exercises across five states in the spring and summer of 2024 to better understand the pathways and plausible evolution of AI-driven election integrity threats, to develop insightful approaches for dealing with these threats, and to facilitate the relationships necessary to do so.
- These tabletops explored eight categories of threats to elections, some posited by BPC and others by the participants themselves. The eight are listed in the chart on the following page.
- This exercise found that, for the most part, AI exacerbates preexisting challenges (such as rumors of election fraud, false information about how to vote, cyberattacks, and other forms of digital sabotage) rather than creating categorically new challenges.
- As such, existing playbooks can be refined or reworked rather than thrown out. The chart on the following page summarizes potential responses to the threats identified during the tabletop exercises.
- Many AI-enabled threats are about communications challenges rather than vulnerabilities in the electoral process itself. These challenges are best overcome by proactively building relationships with stakeholders who can get accurate information out to the public. Because election officials have limited resources, time, and staff, tech companies and other large stakeholders should take on the work of initiating relationships with election offices. Administrators and local journalists should continue strengthening their mutual relationships, and state and federal governments should adequately fund partnership-building efforts across sectors.
- Despite reports of high turnover, election officials have the grit and experience to do the job. Sixty-five percent of election officials have previous experience administering a presidential election. Overall, new chief election officials have an average of eight years' experience running elections and 11 years' among officials in large jurisdictions.
- Transparency and proactivity are key. Even though every crisis may not be foreseeable, having the right plans, processes, and relationships in place to deal with crises can make all the difference. AI can also offer tools for coping with certain challenges.

- These tabletops did not envision any scenario with no solution, but many of the most disruptive possibilities will require judicial remedies. Here, too, officials can work in advance to ensure that judges understand the election process and the rules and procedures governing it.
- This report also outlines recommendations for election officials and other key stakeholders to better prepare for and mitigate crises as they occur, including proactive relationship-building, public communications planning, and leveraging new channels and platforms for information sharing.

Table 1: AI-related Election Threats and Recommendations

Scenario Type	Example of Threat	Recommendations
Synthetic misrepresentation in political messaging	AI is used to make a political figure appear to say something damaging.	Largely outside of election officials' purview.
		Journalists should cover cautiously if at all, perhaps using it as an opportunity to educate audiences about AI.
Misinformation about time, place, or manner of voting	False voting information is spread by AI.	Leverage all partners—government, community, tech, and media—to "flood the zone" with correct information.
	Spoofed websites with misleading information are created.	Work with tech companies to identify, downrank, or remove. Adopt a .gov domain so official information is easily identifiable.
	Misleading claims about polling places or ballot return are made.	Post public notices in facilities like post offices or libraries that are incorrectly identified as polling places.
False claims about election misconduct	Bad actors use AI to fabricate evidence.	Reference previously produced materials about safeguards that invalidate the false claim (e.g., bipartisan staff required to access voting machines, or old ballots ready for disposal are kept separate from current ballots).
	Real footage is misused or Freedom of Information requests are made to fabricate narratives.	Educate journalists and the public on the origin of the footage.
Conspiracy theories capitalizing on human or technical errors	A tabulation error or official mistake is discovered.	Emphasize transparency but investigate before making a public statement to avoid backtracking later. Emphasize that results are unofficial, and discovery of mistakes during this period is part of the process.
	Rumors circulate about a hacked vendor.	Work with the vendor to communicate with the public and test systems for reliability.
Impersonation of election officials	Officials receive fake instructions appearing to be from the state.	Tabletop participants found this scenario unlikely because official channels for policy changes already exist, and peer group chats help officials check in with each other.
AI-facilitated spam or process interference	Officials receive a flood of fake forms or complaints.	Implement "friction" to reduce spam. Seek resources to triage real complaints from fakes and duplicates. Create standard responses to similar complaints. Seek local backups if state databases crash from DDoS attacks.
Security threats to officials, processes, or facilities	Mail-in ballots containing white powder slow the count.	Law enforcement to test safety of ballots; ballots may have to be duplicated to run through tabulator.
	Someone threatens election board members if they certify the election.	Plan in advance with law enforcement and extend dignitary protection teams and other safeguards to officials and their families.
	Rioters breach a tabulation center, compromising the chain of custody.	Check voting machines and scanners for backup data or ballot images. Work with a judge to precertify contingency plans.
Challenges to certification	Rogue election boards refuse to certify the election.	Work in advance to educate the judiciary on election processes so conspiracy theories or non-credible claims can be dismissed quickly in court.

Introduction

An adage holds that 2024 is the United States' first "AI election." Observers fear that AI will pose serious and novel threats to election administration. These fears are not universally shared, but few would entirely write off the possibility of malicious actors using AI to create chaos after a close election.

The Cybersecurity and Infrastructure Security Agency suggests several ways that bad actors could use AI to threaten election-related processes, facilities, personnel, or vendors. Fabulists could use AI to generate photorealistic fake images of election officials mishandling ballots, or they could create compelling video evidence of violence at polling places to deter voters from casting ballots in the first place. Bad actors might, for example, synthesize an official's voice in an advanced spear-phishing attempt. Large language models could generate mountains of burdensome public records requests or fraudulent complaints of irregularities, each demanding precious time from officials. These are only a few of the worries keeping observers up at night.

Election workers already face high, if not unprecedented, levels of stress and scrutiny. They are experiencing a steep increase in false allegations about their work and integrity, harassment and threats to their well-being, and interference from election saboteurs. On top of that, they are training the next cohort of officials after an increase in turnover over the past two decades. Few in the profession have the extra bandwidth to think through the implications of AI for their work.

By working in partnership with other stakeholders—government agencies, private-sector tech companies, and nonprofit advocacy organizations—election workers can better prepare for the threats and opportunities AI might bring. Together, election officials and their partners can claim the rare advantage of strategic foresight: AI risks have risen to the top of the public agenda, and policymakers and other stakeholders are focused on AI to an unusual degree. Concrete action is both necessary and possible.

This report outlines the types of threats most often described in the tabletop exercises, the stakes various actors and sectors have in each, and the types of responses identified by participants. We then make a series of recommendations for stakeholders for the 2024 election and subsequent cycles. Some solutions are simpler than others, and this report will also summarize nuanced discussions about the ease—or difficulty—of implementing the recommendations emerging from the tabletop exercises.

FIVE EXERCISES IN FIVE STATES OVER FOUR MONTHS

In the spring and summer of 2024, the Bipartisan Policy Center held five tabletop exercises to connect state and local election officials with key stakeholders from other sectors and institutions. Together, participants brainstormed ways that election officials could respond to hypothetical scenarios involving AI and the election, and how to manage the resources and relationships they would need.

FIVE TABLETOP EXERCISES IN FIVE STATES:

April: Georgia

May: Pennsylvania

June: Michigan

July: North Carolina
Ohio

These tabletop exercises had four goals:

- to better understand the pathways and plausible evolution of AI-driven election integrity threats;
- to gain insight into how the community might raise the cost of deceptive election-related activity;
- to establish approaches for more rapidly detecting and defusing these threats;
- to build relationships among stakeholders who have a role in strengthening election integrity.

Each exercise focused on a different state. Participants divided up into four teams: one focused on election officials; a second focused on other relevant stakeholders such as journalists and technology companies; a "blue sky" team with permission to imagine unlimited resources for response; and a team of "disruptors" responsible for creating novel scenarios, which were "injected" midway into the discussions.

To encourage frank discussion, these tabletop exercises were held under the Chatham House rule: remarks could be cited but not attributed to any individual participant. As such, this report does not list individual or institutional participants.

The tabletop exercises were intentionally intersectoral; part of their value was to broker introductions and relationships between different types of stakeholders, particularly in recognition that electoral challenges require a whole-of-society response. They included not only elections officials at the local level but also state-level officials and representatives of technology companies, internet security professionals, nonprofit organizations in the elections space, the National Guard, emergency management agencies, and other relevant stakeholders.

The Scenarios: Categorizing Election Threats

SYNTHETIC MISREPRESENTATION IN POLITICAL MESSAGING

Several scenarios involved the use of synthetic media—fake images, video, or audio—in political messaging to misrepresent a candidate or another person. A candidate or their representative might be made to appear to have done or said something damaging that they did not do or say; candidates or local surrogates could even lend their likeness to digital avatars who hold virtual rallies for supporters.

Participants quickly dismissed these scenarios as outside the purview of election officials. Their job is not to influence *how* people vote, but rather to ensure they can exercise their right to vote if they wish to do so. Weighing in on the veracity of campaign communications would appear partisan; officials agreed that in these scenarios, they should "let the marketplace" of ideas run its course.

Other stakeholders had more leeway to act. Participants said they hoped journalists would use these scenarios—if they covered these events at all—as opportunities to educate the public on AI, how it is used, and how they can verify the authenticity of information. Tech companies, each of which has their own distinct policies on how synthetic media may be shared on their services and what happens when those policies are violated, also acknowledged that they have a role to play by enforcing those policies.

CATEGORIES OF ELECTION TABLETOP SCENARIOS:

1. Synthetic misrepresentation in political messaging
2. Misinformation about time, place, or manner of voting
3. False claims about election misconduct
4. Conspiracy theories capitalizing on human or technical errors
5. Impersonation of election officials
6. AI-facilitated spam or process interference
7. Security threats to officials, processes, or facilities
8. Challenges to certification

MISINFORMATION ABOUT TIME, PLACE, OR MANNER OF VOTING

Election officials were quick to agree that they do have a stake in correcting false information about the time, place, or manner of voting. Such misleading information has circulated in previous elections—if not since the dawn of American democracy—but AI can be used to create it quickly at a high volume or to better tailor it to specific audiences. The opportunities for mischief were many. Scenarios included:

- AI-created synthetic content suppresses votes by spreading rumors of violence at local polling places.
- Fake websites are circulated, with credible URLs containing misleading information about polling place locations or hours.
- WhatsApp, QR code, or some other medium are used to spread voting misinformation in non-English languages.
- AI-generated text messages tell voters that a technical error resulted in their mail-in ballot being invalidated.
- A misleading video falsely informs voters they can return their ballot at the library, leading to mass confusion.

The watchwords for responding to these scenarios were "partnerships" and "communication." The best approach is, when possible, proactive communication of accurate information, or "flooding the zone" with truth. For this reason, it is important to establish early on in citizens' minds where they can go for authoritative information.

Survey research by BPC shows that voters go to different sources for different types of election information. For information about the time, place, and manner of voting or about election administration more generally, they are more likely to consult local election offices. This is why it is important for election offices to register for a .gov web domain: It gives voters a simple way to verify that they have reached the authentic, authoritative source, and not an imposter spreading incorrect instructions. Election offices' social media presences should also be verified to the extent possible through account badges or other identifiers. Social media companies should take measures to authenticate these accounts when possible, with help from state and federal agencies.

When it comes to election-related commentary or news about results, BPC's survey research shows that voters are more likely to consult online search engines or news media. This is one reason relationships between media and election offices are so important: Officials can improve reporting and elevate correct information by providing it to journalists before coverage begins.

Partnerships and communication are just as important when being proactive is not possible and officials must react instead. Election officials might work with law enforcement and tech companies to restrict (or even de-host) fraudulent websites, for example. These relationships are best developed in advance; in an emergency, it may prove too difficult to reach the correct representative from a tech company. Journalists, too, are more likely to turn to election officials to debunk rumors and get accurate information if they have a preexisting relationship.

What about "demotivational content"?

There was some discussion—but not a clear consensus—about how election officials should respond, if at all, to "demotivational" content discouraging voters from participating in an election. Although they agreed that election officials should not correct false partisan statements, some officials do believe they should encourage the public to vote. Officials also noted that the individuals most likely to be affected by voter suppression efforts tend to be from minority or low-income backgrounds. These officials suggested that as part of their goal to be a trusted voice on election-related issues, election offices should encourage voters to be tech and media literate and to think critically about election-related claims.

FALSE CLAIMS ABOUT ELECTION MISCONDUCT

In the past, election officials and their conduct have been the targets of rumors and false allegations. Ruby Freeman, for example, was a Georgia election worker who faced online harassment after conspiracy theorists wrongly claimed she was complicit in fraud in the 2020 election.

In 2024, newly available AI tools can be used to fabricate evidence in support of similar claims. Tabletop participants considered various scenarios, such as the manipulation of footage from body cameras worn by election workers to give the impression ballots were mishandled, or the combination of synthetic audio and footage from a tour of a storage facility to create the illusion of election officials admitting to fraud.

AI is not necessary to create these narratives—past incidents have simply taken publicly available security footage out of context, for example showing election workers disposing of old ballots and alleging votes were being thrown out. But AI does allow for easier fabrication of such "evidence."

Participants in tabletop exercises treated these scenarios like exercises in crisis communications. They advised a rapid response to these claims, perhaps through press conferences on local TV and briefings for local reporters. Officials might reference previous efforts to educate the public and media about election safeguards, such as requirements that ballots be handled by both a Democrat

and a Republican. They can also point out inconsistencies between fabricated evidence and election processes: Old ballots ready for disposal are stored in different bags and areas than ballots to be tabulated, for example. Officials in certain states can also point to mandatory postelection audits—which the public can sometimes observe—to reassure voters.

The Elections Group offers several resources to officials looking to expand or improve their auditing and administrative processes. Consider:

- a series of comprehensive guides on audits for ballot management, ballot proofing, mail ballot validation, vote tabulation, and voter list maintenance;
- reporting templates for risk-limiting audits, fixed-percentage audits, and automated audits;
- audit report inserts showing checklists of best practices;
- a template for a handout informing voters about audit processes and best practices;
- templates for talking points when presenting audit results;
- a template for a press release reporting on audits.

CONSPIRACY THEORIES CAPITALIZING ON HUMAN OR TECHNICAL ERRORS

Elections are complicated processes. Despite the many redundancies and safeguards in place, election workers are human and errors are inevitable. When they occur, it takes time to identify the source and correct them. In 48 states, postelection audits are held to verify the integrity of the process.

During the tabletop exercises, it quickly became clear that AI-enabled threats of this type are, as with so many other threats, about communication challenges rather than vulnerabilities in the electoral process itself. The period of time between discovery and correction of an error is vulnerable to rumors and spurious allegations of impropriety. Artificial intelligence allows bad actors to take advantage of this vulnerability quickly and to produce a greater volume of content than before. Many scenarios focused on the possibility of an error—a misprogrammed ballot scanner, for example—and how election officials should balance the imperative of transparency with the need to defend public confidence against false claims of fraud.

The manner in which an error is initially disclosed is crucial, and it helps to have a crisis communications plan in place *before* something happens. Even if reports of an error are false, a categorical denial is often inadvisable. Mistakes do happen—election officials have tabulated votes early or incorrectly, for example. In such moments, quick disclosure with careful messaging is key. Participants said that in the past, they have stressed that initial results were unofficial tallies and the fact an error was caught *before* certification meant that the system was working as designed. They also reported working directly with journalists to make sure the intricacies of the election process were reported accurately.

Materials explaining the process in advance can become valuable references for officials looking to prove that they have nothing to hide. Preemptive warnings to the public that it would take time to process absentee ballots in 2020—and that results might be delayed as a consequence—were cited as proof of concept for this "pre-bunking" approach.

Responding to potential errors by vendors can be less straightforward for election officials. One scenario, for example, asked participants to suppose that rumors arose claiming a voting system provider had been hacked. Rumors can be nearly as disruptive and damaging to public confidence as an actual hack, because officials have no way to prove with certainty that a provider was *not* hacked. Reassuring skeptical members of the public or election boards might require re-running ballots with a verified "clean" copy of tabulation software and conducting a manual audit to verify a correct count.

As with the examples above, this time-consuming process would likely be a breeding ground for rumors. Election officials can be transparent about what they know and are doing in response, but as private contractors, vendors might not. Participants were unsure if they could somehow require vendors to be more proactive on public communications in the event of a potential compromise; some wondered whether language to this effect could be inserted in contracts with state and county governments.

At no point did any scenario present an error or technical failure so severe that the election results became unknowable. After all, 95% of voters in 2024 will probably cast ballots with a voter-verifiable paper trail rather than a direct-recording electronic voting machine. This is a result of the many redundancies and fail-safes built into election systems. For example, when asked to consider a failure of the secretary of state's voter registration database during the cure period for provisional ballots, participants noted that county governments keep backups of that database and that while such an issue would slow down the count, officials could work together to continue processing provisional ballots.

IMPERSONATION OF ELECTION OFFICIALS

Some scenarios asked participants to consider the potential impact of a fake communication from a state official (usually the secretary of state). The official might give incorrect instructions, such as announcing a major change to the way provisional ballots are cast or counted.

Election officials were quick to dismiss these scenarios because major policy changes are not announced by a personal phone call. Some said they would not believe such a call until it had been verified in a group chat with officials from other jurisdictions.

A more likely scenario is that a lesser-known figure, such as a local official, is impersonated in a call to temporary poll workers. Both the secretary of state scenario and this possibility demonstrate the value of well established chains of communication—vertically, so that official communiques from above come in familiar formats via predictable, verifiable channels; and horizontally, so that election officials can verify information and request advice from their peers.

AI-FACILITATED SPAM OR PROCESS INTERFERENCE

The tabletop exercises proposed several scenarios in which malicious actors could use AI to facilitate interference in the election process through spam or to interrupt and delay officials' work.

For instance, bad actors could use AI to generate a huge volume of complaints to election offices, creating large backlogs that overwhelm staff. When asked to consider this scenario, participants said it was likely to happen and that the best response would be to find some way to handle the volume of incoming complaints while continuing their essential work. One participant said they route email complaints to a special inbox so that they can be replied to in batches; another said they had explored software to help them to respond automatically. When smaller offices receive too many complaints that appear coordinated, some simply prioritize their other work instead of trying to answer every phone call. Participants also considered ways of adding "friction" to the complaint process, such as requiring users to provide some kind of personal identifying information or to pass a CAPTCHA test.

Participants noted that if AI were used to generate a large volume of a similar complaint or request (for example, a registration cancellation form for real voters), they would note the atypical increase in such a communication from voters. This would tip them off to consider responding to the request as they would a threat by evaluating its authenticity and referring the matter to the secretary of state's office or federal law enforcement for investigation.

If voters themselves are duped by false information (in one scenario, for example, a claim their absentee ballot could not be counted) and call the election office in response, participants said they have ways to respond without stopping work to answer every phone call. Responses can be recorded on voicemail lines, or officials can communicate a correction directly to registered voters who provided their email information or utilize a county emergency message system to reach the public. Relationships with media would also be useful here, as officials could tell local reporters what is happening and ask them to help share accurate information with the public.

SECURITY THREATS TO OFFICIALS, PROCESSES, OR FACILITIES

Many of the most alarming scenarios discussed during the tabletop exercises involved some kind of security threat or breach. AI might be used to deliver these threats or motivate individuals to carry them out, but as with other scenarios, this technology is not strictly necessary to generate them.

In fact, one scenario threatened to delay certification by causing chaos without the use of AI at all: What if someone placed ballots containing an innocuous white powder, such as baking soda, in drop boxes? Although the U.S. Postal Service tests mail for hazardous substances, ballots delivered by drop box bypass this process. A county office might have to delay counting results until the ballots could be deemed safe to handle. Once that happens, they would also have to be duplicated in accordance with rules on ballot spoilage because ballots covered in powder cannot be run through tabulation machines.

Other scenarios raised the specter of violence against officials. One asked participants to consider threats against election boards on the date of certification—a meeting at which members would all be in attendance in a publicly known location. Another asked participants to consider what might happen if AI-generated phone calls delivered personalized threats to election officials and their families, or to board members warning them not to certify the election.

The latter was especially chilling because in some jurisdictions, board members are required to physically gather at a specific time and publicly accessible place, leaving them vulnerable to potential violence. County governments and law enforcement might need to be on standby with bomb-sniffing dogs, hazardous material suits, and other equipment to verify the safety of facilities. In extreme circumstances, they might also need to consider deploying “dignitary protection units” to guard the safety of officials and their families.

Participants warned that many emergency response exercises also involve threats to one polling place or precinct—for example, if someone were to call in bomb threats to *every* polling location or precinct, a massive government response would be needed. Officials should plan for these kinds of extreme threats just in case.

What if there is a catastrophic security breach?

Perhaps the most dramatic scenario asked participants to imagine a protest outside a tabulation facility that devolved into a riot, leading to a security breach while workers were counting ballots. If ballots and the USB sticks on which results are reported are in the same facility when this happens, it may become difficult to maintain and verify the chain of custody. One participant remarked that if these materials were destroyed or stolen, it would be as if an act of domestic terrorism had disrupted the election.

There are defenses against an event like this. Many facilities have doors that are double-locked, requiring badges from a Republican and Democratic staffer to enter. Many counties keep local backups of vote tabulation totals on individual ballot scanners, which would allow the results to be regenerated. (One official was surprised to learn that their machines likely had this capability, signaling that refresher training on the safeguards built into election devices is important.)

If those defenses fail, it would lead to an emergency not dissimilar to the plot of a recent television drama. Participants began brainstorming how they might determine if any ballots were lost or destroyed (because there should be a record of the total number of ballots cast), and how they might identify voters whose ballots were not recoverable and might be included in a potential revote. These unusual remedies would almost certainly end up before federal courts, or even the Supreme Court. Election officials said that because of the high degree of scrutiny they would face, they would welcome judicial oversight in these circumstances, and they might even work with the judiciary in advance to explain their strategy and ask if the courts could approve it in advance.

CHALLENGES TO CERTIFICATION

A final category of scenarios asked participants to consider the possibility that election boards or state bodies might refuse to certify the election results. Election certification is generally a ministerial duty—it is a mandatory task that is not up to the discretion of officials and typically involves only validation of the vote count, not investigation of the election's conduct. Reforms to the Electoral Count Reform Act also clarify and strengthen processes for adjudicating exactly this type of dispute. But if boards refuse to certify the results, the delay would last until a judicial decision and create another window of vulnerability and lend credibility to false claims of fraud. This scenario would be a dangerous place for American democracy to find itself.

Key Lessons and Recommendations

Despite the generally high level of anxiety about threats to the 2024 election, our tabletops led to the encouraging conclusion that new technological risks like artificial intelligence do not always require complicated new solutions. Previous forms of response—such as rapid communications playbooks, basic cybersecurity improvements, strong relationships with local partners, and emergency contingency plans—do not need to be wholly reinvented, just revisited.

The dark side of this conclusion is that many of the most alarming scenarios only minimally involved AI—and were plausible without it. Rumors of election fraud may or may not need AI's assistance to inspire a riot at a tabulation facility, for instance; after such a riot, AI may or may not be used to spread additional rumors about the aftermath.

Drawing on the discussion above of the different types of scenarios, the remainder of this report makes several recommendations for stakeholders preparing for Election Day both in this cycle and in years to come.

BUILD NETWORKS OF RELATIONSHIPS BEFORE YOU NEED THEM

Many of the scenarios discussed posed communications-related challenges not dissimilar from those in previous cycles: false claims of election fraud, a skeptical or angry public, or the possibility of human error being seized upon and cast in a sinister light.

Artificial intelligence threatens to magnify these challenges, but not to change their fundamental nature: Proactive relationship-building and strategic communication remain the best responses. This sounds simple, but most election offices are already strapped for time, staff, and resources. It was only in the past several years that many officials began to consider public communications about election integrity a primary function of their job. In this cycle, as in the past, outside stakeholders have sought to ease this burden by providing free resources (planning checklists, social media post templates, crisis communications guides, etc.) for election officials. And as BPC's research shows, election offices struggle to compete for voters' attention and trust with limited resources in today's crowded media environment.

This is why relationship-building with other stakeholders is so important: It allows officials to augment their efforts. Over and over during the tabletop exercises, participants returned to the theme of "early and strengthened" relationship-building. They recognized the need to have these relationships in advance so that officials can "activate" networks of necessary partners in moments of need.

Crucially, the goal of most election officials' communication is not to dissuade hard-core conspiracy theorists—something that is likely far beyond their means to achieve. Instead, election officials should think about their communications as reinforcing the confidence of the crucial, but less vocal, swayable middle.

LEVERAGE THE FULL RANGE OF PARTNERS AND CHANNELS

Participants discussed leveraging other county and municipal government offices, including local mayoral offices, public libraries, inserts in water bills, SMS messaging over emergency alert systems, and the many other touchpoints citizens have with local government.

Journalists are another important potential partner. Unfortunately, the decline of local media in recent decades leaves fewer print journalists (and readers) than before. Television stations have become an important alternative, and election officials are strengthening their relationships with TV journalists, making sure they understand how the voting and tabulation processes work so that they do not incidentally end up giving unfounded rumors more airtime or credibility than they merit.

Other local actors who have strong credibility with the public or specific communities are also valuable partners, even if they are not traditionally part of the election process. Participants discussed working with local churches, veterans' groups, and firehouses, for example, since much of the public considers pastors, veterans, and firefighters to be credible messengers. County and local party chairs can also

In August 2023, the U.S. Election Assistance Commission published an "AI Toolkit for Election Officials." It includes basic information about threats and opportunities from AI for election administration, as well as tips on how to communicate with the public:

1. Communicate clearly and concisely about voting rules and processes.
2. Meet voters "where they are" by providing information in formats they are likely to consume, such as social media or informational mailers.
3. Provide customer service training to poll workers to smooth the voting process and build public trust.

be a resource: Leveraging their bipartisan nature, election officials can get word to voters across the political spectrum through relationships with party chairs.

Some suggestions were ambitious and creative. One blue sky team, for example, suggested massive messaging campaigns with TV and billboard advertising. Another participant proposed printing voting information on the wrappers at local sandwich shops.

HAVE A PLAN FOR COMMUNICATING IN CRISES AND AFTER ERRORS

Not every scenario can be planned for in advance. Things can and will go wrong in unexpected ways. Participants made several observations about how they handle unexpected crises, errors, or setbacks in election administration when they are under fierce public scrutiny.

Transparency was a primary theme, but participants cautioned that officials should "investigate and diagnose" before getting behind a microphone and addressing the public or the press. A hasty denial or mistaken diagnosis requiring officials to backtrack could be more damaging than any delay. Participants also recommended advising the press and other parties that the investigative process takes time, and that the unofficial results stage catches errors.

So much of public reassurance in these moments relies on education about the election process, both for journalists and the public. Even in an unforeseen crisis, resources created in advance of the election can be a valuable resource: As one participant put it, they have "longevity" that makes their explanations for process safeguards more credible. By this logic, election officials can prepare for crises or mistakes by preproducing materials about mail-in voting, the tabulation process, logic and accuracy testing, postelection audits, and other elements of the process.

PLAN FOR ACCESSIBILITY ISSUES

Some participants noted that significant populations in the United States still do not have internet access, especially broadband internet access. Online video statements and informational materials are unlikely to reach these voters, and thus officials should not overlook traditional forms of information sharing.

Smaller election offices might also struggle to provide information in languages other than English. Larger counties often have the resources to translate materials and communicate with voters in their native languages, but smaller election offices often rely on Google Translate and similar tools. Because some of the scenarios in the tabletop exercises involved false information about voting in Spanish or other non-English languages, participants stressed the

need to build relationships with leaders of large communities of non-English speakers. “I would go straight to the priest at our local Hispanic Catholic church,” said one.

ESTABLISH SIGNALS OF CREDIBILITY

One of the simplest defenses against misleading sources of information about voting is to establish a signal of credibility for authentic communications; most often, this means a .gov web address for election offices. A 2024 BPC analysis found that only 31% of election office websites use .gov. Instead, most websites use .com, .net, or .org domains. Anyone can purchase websites with these domains, meaning that it is easy for a bad actor to credibly impersonate election officials. Election officials who have not made the move to .gov may share control of their web presence with local or county officials, may not have dedicated IT staff to manage this transition for them, or may face financial barriers. For instance, if their web address is prominently displayed on government vehicles, it would necessitate an expensive design change.

Other useful but less frequently discussed signals of credibility include verifying social media accounts on X, Facebook, Instagram, and other platforms, and the creation of a three-digit telephone number for all election-related communications.

STRENGTHEN AND CENTRALIZE GOVERNMENT RELATIONSHIPS WITH TECH PLATFORMS

State and federal government agencies could do more to work with tech companies to provide these and similar solutions. For example, a standardized verification badge for government accounts across platforms would improve visibility for the public. Rather than attempting to watermark AI-generated content with provenance data, priority could be given to watermarking official government communications so they can be more easily verified with greater confidence.

In general, having federal and state officials interact more often with tech companies on behalf of local election officials can be beneficial. Tech companies sometimes struggle to maintain relationships with the large number of elections offices around the country, leading to service issues. For example, one participant said they needed to submit an ID five times before Facebook verified their official account. State governments and federal bodies like the Election Assistance Commission and professional organizations like the National Association of Secretaries of State, the National Association of State Election Directors, and the National Association of Election Officials are often able to get in touch with tech companies more quickly.

Creating more standard and centralized channels (such as the Elections Infrastructure Information Sharing and Analysis Center, or EI-ISAC) for these kinds of basic processes might help.

Another potential step toward empowering states to more actively manage relationships with tech companies is the creation of "misinfo [at]" email addresses for state election bodies. Participants envisioned these functioning essentially as hotlines, helping states to identify false information about voting quickly and encourage platforms to take appropriate policy enforcement actions when relevant.

BUILD RELATIONSHIPS WITH LAW ENFORCEMENT IN CASE OF EMERGENCY

The most frightening scenarios typically involved election-related violence, threats of violence, or other physical safety risks. Many offices have emergency response and contingency plans to protect personnel and continue operations in the wake of a security incident or weather event. These plans often include steps to improve security for themselves, their teams, and their facilities by using, for example, panic buttons for precinct site supervisors or shatterproof glass on windows. They also typically involve establishing preexisting arrangements with local law enforcement: Offices could have the sheriff on standby, or ask police to incorporate polling places into their patrol route.

When faced with scenarios describing catastrophic failures or extreme threats, participants began brainstorming further preparations. Officials could, for example, give law enforcement contact information for every precinct site supervisor to improve communication and response times. The best time to have these conversations is early, before police intervention is needed.

CONSIDER THE JUDICIARY A STAKEHOLDER, TOO

Some scenarios, such as those involving boards of elections refusing to certify results, were beyond the purview or influence of election officials to resolve. Although participants always came up with solutions to the challenges posed by the scenarios, those solutions often depended on the judiciary to approve emergency measures or overrule rogue election boards. These fail-safes come with huge risks to public perception. As one participant put it, "Everything has a legal solution, but there are many news cycles between an event and that solution."

To prepare for the unfortunate but very real possibility of court involvement, some participants suggested that future election integrity exercises involve judges and clerks. Although the decisions are ultimately up to courts, educating the judiciary on election procedures and preclearing contingency plans for continuing operations or correcting errors can ameliorate legal challenges later.

EXPLORE POSSIBLE BENEFITS FROM AI FOR ELECTION ADMINISTRATION

Finally, while our tabletop exercises focused mostly on AI threats, some participants said that election officials should explore ways AI can improve their processes and ease the demands on their staff. Some participants admitted to not having considered this possibility, suggesting a future opportunity to improve election administration. Examples of beneficial use of AI include enhanced and more efficient training of poll workers; signature matching tools; proofreading election materials and communications; and helping to identify potential polling locations based on traffic patterns and other data. When considering or implementing AI tools for these or other purposes, it is essential for officials to include a human in the workflow for quality assurance purposes and to think carefully about ethics and equity implications.

Conclusion

At the time of this report's publication, the 2024 election is just weeks away. Professionals across sectors are at various stages of implementing measures like the recommendations above. Voters are already casting early and mail-in ballots.

Despite reports of record turnover in the profession, there are reasons to be optimistic about the level of preparation among election officials. BPC research has found, for example, that 65% of local officials have experience running a presidential election. What is more, the new officials hired to replace outgoing officials are not greenhorns; they have an average of eight years of experience running elections. In large jurisdictions, that number rises to 11 years.

Although time remains for election officials to make final preparations before the November election, the recommendations in this report will likely hold for future cycles. The current political climate of public distrust, affective polarization, and partisan vitriol shows few signs of abating. Artificial intelligence will likely become both more powerful and more accessible to consumers. Although the 2024 election cycle already stands out as historic, in the months and years following, officials will do well to reflect on lessons learned and how to prepare for the next election—which is always just around the corner.

Bipartisan Policy Center

1225 Eye St NW, Suite 1000
Washington, DC 20005

bipartisanpolicy.org

202 - 204 - 2400

Policy Areas

- Economy
- Energy
- Human Capital
- Health
- Housing
- Democracy

The Bipartisan Policy Center helps policymakers work across party lines to craft bipartisan solutions. By connecting lawmakers across the entire political spectrum, delivering data and context, negotiating policy details, and creating space for bipartisan collaboration, we ensure democracy can function on behalf of all Americans.

@BPC_Bipartisan
facebook.com/BipartisanPolicyCenter
instagram.com/BPC_Bipartisan
linkedin.com/company/bipartisan-policy-center

Bipartisan Policy Center

1225 Eye Street NW, Suite 1000
Washington, D.C. 20005