POLICY REPORT

BRENNAN CENTER FOR JUSTICE

Securing the 2024 Election

Recommendations for Federal, State, and Local Officials

By Derek Tisler and Lawrence Norden PUBLISHED APRIL 27, 2023

Brennan Center for Justice at New York University School of Law

Table of Contents

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform and revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at
www.brennancenter.org

Introduction

What are the gravest threats to the security and integrity of U.S. elections? Over the past decade, the answer to that question has evolved. In addition to foreign cyberattacks and influence campaigns, dangers such as intimidation of election workers and conspiracy theorists assuming election administration positions now put U.S. democracy at risk. In the lead-up to the next presidential election, the United States must adjust to this changed landscape and ensure that the democratic process is protected when the nation goes to the polls.

In 2016, Russian cyberattacks on election infrastructure highlighted the need to strengthen the resilience of U.S. election systems. As a result, the Department of Homeland Security (DHS) designated election systems as critical infrastructure,[1] and federal, state, and local officials worked together to reinforce them against cyberattacks. New threats, largely stemming from amplified efforts to fuel distrust in U.S. elections via the spread of election falsehoods, must be met with the same urgency.

The deliberate spread of election falsehoods — including denial of the 2020 presidential election results — culminated in the attack on the U.S. Capitol in 2021 that President Donald Trump instigated in an attempt to overturn a free and fair election. It has also led to serious challenges to the integrity of future elections, including partisan interference in election processes, intimidation and violence against election workers, and the risk of insider attacks in which the very government workers tasked with administering U.S. elections directly endanger election security. Since the 2020 election, advances in artificial intelligence (AI) have made it possible to produce vast volumes of text peppered with falsehoods; generate convincing deceptive images, video, and audio; and distort public figures' words and actions at a previously unseen scale. These threats are likely to grow ahead of 2024. Powerful politicians, including presidential candidates, and national pundits continue to encourage disruption of the election process and cast doubt on results.

Abroad, U.S. elections have become a battlefield in the conflict over the global order. Heightened stakes in Ukraine and other flash points have increased the motives for powerful countries to interfere in future contests. The Office of the Director of National Intelligence recently warned that the Russian government "views U.S. elections as opportunities for malign influence as part of its larger foreign policy strategy," and the Kremlin continues to look for ways to undermine American democracy.[2]

Not only have foreign and domestic threats to American elections evolved and metastasized but they also fuel one another. In 2020, election falsehoods were mostly spread by domestic political actors, who used tactics similar to those that Russia exercised four years earlier, while Russian agents amplified these lies.[3] After the election, Iranian operatives drew on the anger some Americans felt about the outcome to incite violence against election officials.[4] Even if foreign cyberattacks are not technically successful, they can still exacerbate domestic distrust of elections.[5] In fact, foreign actors do not even need to attempt a cyberattack to cast doubt on election security, as Iranian operatives demonstrated in 2020 with a video that created the illusion that someone had hacked a state voter registration system.[6]

Taken together, these trends have rendered U.S. election systems increasingly vulnerable. Over the next 18 months, policymakers must address four overlapping threats to election security: the spread of false information to undermine election results and prevent citizens from voting; harassment, intimidation, and physical violence against election workers and officials; insider attacks; and cyberattacks against election infrastructure.

These challenges require a whole-of-government response. At the federal level, DHS — in particular, its Cybersecurity and Infrastructure Security Agency (CISA), which defends and secures the nation's critical infrastructure — along with the Election Assistance Commission (EAC), the FBI, and other federal agencies should direct more resources to combat these threats. Additionally, the Department of Justice (DOJ), via its task force on election threats, should bolster its relationships with and provide further guidance to local law enforcement and election officials.

State legislatures should make it easier for officials to combat election lies, protect election workers, prevent insider attacks, and guard against cyber threats. New laws should give election officials more flexibility to count ballots faster, expand protections for elections workers, and outline restrictions to safeguard election systems from tampering and unauthorized access.

Finally, state and local election officials should expand their efforts to protect elections, including preempting misinformation with official web pages that disprove rumors about election systems; adopting measures to prevent, detect, and respond to insider threats; and creating contingency and communications plans in the event of a cyberattack.

The time is now to defend the election process against future threats. American democracy depends on it.

TABLE 1

Key Recommendations for the Federal Government, State Legislatures, and State and Local Election Officials

THREATS	FEDERAL GOVERNMENT	STATE LEGISLATURES	STATE AND LOCAL ELECTION OFFICIALS
Spread of false information	■ CISA should share best practices for strengthening societal resilience to the spread of false election information — including falsehoods generated by AI — and promote the dissemination of accurate information from election officials, including through public-private partnerships. ■ CISA should escalate efforts to help local officials adopt and transition to .gov domains for election websites. ■ The EAC, working with CISA, should build public awareness and confidence in voting system security.	■ Mandate that local election offices use .gov domains. ■ Prohibit the spread of materially false information concerning the time, place, or manner of voting with the intent to prevent voters from exercising their right to vote. ■ Allow earlier processing and counting of mail ballots.	■ Dedicate resources to anticipate and refute false election information through public outreach.
Harassment and threats of physical violence	■ CISA should increase resources to protect election workers and sites, including by establishing regional election leads and increasing the number of protective security advisers (PSAs). ■ DHS should continue to require states to spend a portion of homeland security grants on election security, as it did in 2023. ■ DOJ's election threats task force should expand coordination with local election officials and law enforcement and reduce barriers for reporting threats.	■ Fund physical security protections and training. ■ Allow election workers to protect personally identifiable information. ■ Prohibit intimidation and doxing of election workers and ensure that all workers receive protection throughout the entire election process.	■ Direct federal grant funding to physical security needs. ■ Improve election workers' access to address confidentiality programs. ■ Provide training on protecting personal information.

Continued on next page

Continued from previous page

THREATS	FEDERAL GOVERNMENT	STATE LEGISLATURES	STATE AND LOCAL ELECTION OFFICIALS
Insider threats	■ CISA should expand its insider threat services by creating additional best practice checklists, developing self-assessment tools, and training PSAs on these materials.	■ Limit access to critical election infrastructure to officials and others needed to ensure that those systems function. ■ Establish authority to prohibit individuals who violate election laws from administering elections and to decommission jeopardized equipment. ■ Require election officials to use voting machines for initial ballot counts in all but the smallest jurisdictions, followed by bipartisan hand-count audits.	■ Develop regulations, protocols, and training to prevent, detect, and respond to insider attacks.
Cyberattacks	■ DHS should ensure that a portion of State and Local Cybersecurity Grant Program funding is set aside for election security. ■ CISA should increase resources to protect election systems, including by establishing regional election leads and hiring additional cybersecurity advisers (CSAs). ■ DHS, DOJ, CISA, and the EAC should educate election officials on federal grant opportunities and help direct funding to the areas of greatest need.	■ Fund the replacement of outdated election systems. ■ Mandate robust postelection audits. ■ Launch cyber navigator programs to help local jurisdictions defend against cyberattacks.	■ Adopt backup systems that allow voting to continue in the event of technical failures or resource shortages. ■ Develop and promote resources to improve the implementation of contingency plans.

I. Combat Election Falsehoods

After the 2020 election, then President Trump and other prominent politicians and public figures conducted a sustained campaign to attack the bedrock of democracy by promoting false election claims, which were then amplified by foreign adversaries looking to damage confidence in American elections.[7]

These deceptions contributed to plunging levels of trust in elections, extraordinary threats against election officials, and a flood of election worker exits.[8] Lies propagated by President Trump and other high-profile election deniers precipitated an insurrection attempt at the U.S. Capitol on January 6, 2021. Looking forward, advances in AI technology could be weaponized to produce deceptive social media posts, messages, images, and videos on a more massive scale and with a greater level of ostensible credibility in the 2024 election. Falsehoods about the election process intended to trick people out of voting — unfortunately a long-standing feature of the U.S. election landscape — compound the dangers of election denialism.

While the pall on democracy cast by election lies may seem like an intractable problem, all levels of government can take proactive steps to curtail the harm. Among other efforts, federal and state governments can work together to encourage local election offices to use .gov domains so the public can easily distinguish official election websites from spoofed ones. State legislatures can pass laws to reduce the spread of false claims about the election process that threaten to suppress the vote, and they can accelerate mail ballot counts to limit rumors from spreading in the uncertain period before election results are certified. And federal agencies, election officials, and civic groups can build the public's resilience by taking action to anticipate and rebut common false narratives about elections.

Curb Deceptive Practices

Lies about how, when, and where to vote — often targeted particularly at Black and Latino voters — have long been used to trick Americans out of voting, especially in the final days leading up to an election.[9] These falsehoods have historically circulated through flyers, phone calls, and other means; in recent years, social media and methods of digital deception, such as the hacking and spoofing of official election websites and accounts, have greatly expanded their reach. These methods are bound to become more sophisticated over time.

>> With federal and state assistance, election offices should transition their websites to .gov domains.

Election websites give voters essential information on voter registration, mail ballot requests and processing, residency and ID requirements, polling site locations and hours, and other election issues. Fake election websites intended to deceive and disenfranchise voters use broadly available .com or .org domains that appear to represent local election offices.[10] During the 2020 election, the FBI identified dozens of duplicitous websites mimicking federal and state election domains.[11] The FBI and CISA have specifically warned that foreign adversaries use spoofed websites as a tool to spread and amplify false claims about elections.[12]

To guard against spoofing and interference, federal and state governments should work together to ensure that election offices adopt .gov domains — which only verified U.S.-based government entities can use — for their websites. When users see .gov in a website URL, they can be sure that they are visiting a trusted government source.[13] Adopting .gov domains would allow users to differentiate more easily between real and fake election office websites. Only one in four election websites currently uses a .gov domain.[14]

CISA, which administers .gov domains, should stress the government domain's national security importance in its messaging to election offices. It should also conduct more outreach to election officials through the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), an organization that shares election-related cyber defense resources among election officials and cybersecurity professionals.

States should require local election offices to use .gov domains, either by statute or, where authorized, by regulation or directive (as Ohio Secretary of State Frank LaRose did in 2019).[15] Doing so would facilitate the transition for election officials who do not control their own websites and are dependent on their counties or municipalities for IT support. Registration for .gov domains is now free for election offices verified by CISA.[16] And states and localities can use federal funds from DHS's newly launched State and Local Cybersecurity Grant Program (SLCGP) for other costs associated with transitioning to new domains. In creating the grant program, Congress explicitly referred to "the delivery of safe, recognizable, and trustworthy online services . . . including through the use of the .gov internet domain."[17]

>> State legislatures should pass laws to curb the spread of materially false information intended to disenfranchise voters.

States should pass laws to prohibit individuals from disseminating materially false information regarding the time, place, or manner of an election or the qualifications

for voter eligibility with knowledge that the information is false and with intent to prevent or deter a voter from exercising their right to vote. Such laws should cover the immediate window before an election — such as within 90 days of Election Day — and be narrowly tailored to address deliberate lying about voter eligibility or voting locations, methods, and times with the intent to disenfranchise voters.

States should also create a private right of action that allows affected voters and other aggrieved parties to sue individuals who violate this prohibition for preventive relief against ongoing efforts to deliberately spread election falsehoods. The laws should further authorize state attorneys general to bring civil enforcement actions against violators to prevent the continuing spread of false election information. To help provide more immediate relief, state laws should allow members of the public to report violations to the state attorney general and should require the attorney general to take reasonable steps to correct the materially false information if the office receives a credible report that an individual or entity has violated the law. The corrective actions should include, where appropriate, written and electronic communications, public statements, and the use of emergency alert systems that reach those exposed to deceptive claims.[18]

Some states have passed or are considering bills that would target deceptive election practices. Kansas, Minnesota, and Virginia already bar the knowing spread of materially false election information about the time, place, and manner of elections that is intended to block votes.[19] Mississippi, Minnesota, and New York have considered bills for the 2023 legislative session that would further hinder specious election claims, and Michigan legislators have plans to introduce a bill with similar provisions.[20]

Speed the Counting of Mail Ballots

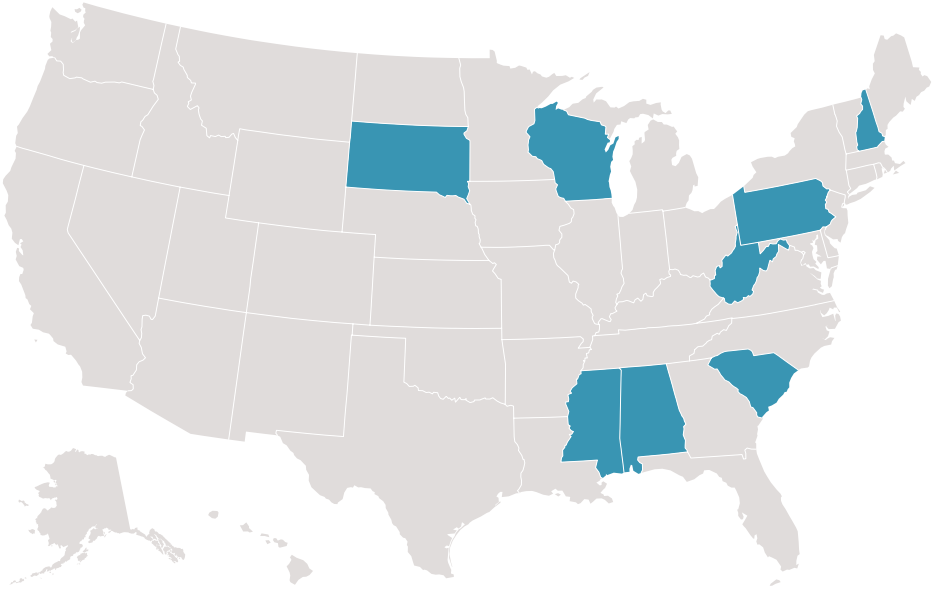
When the demand for accurate information on an election topic outpaces the supply — as can happen when the public needs to wait for ballots to be counted to learn the outcome of an election — false narratives can seep in and fill the resulting information vacuum. After many states expanded mail voting access in 2020 due to the Covid-19 pandemic, then President Trump and other prominent election deniers exploited an underinformed public by attacking the mail voting process and sowing election lies in the fertile ground of uncertainty.[21] With Republicans urging voters not to vote by mail, mail ballots skewed Democratic; as a result, the slow count of mail ballots superficially seemed to change the direction of race outcomes — an especially strong focal point of election conspiracies.

>> State legislatures should allow and expand preprocessing of mail ballots.

This lengthy delay in result reporting and consequent cycle of mistrust is not inevitable. Ahead of Election Day,

FIGURE 1

States That Do Not Allow Any Preprocessing of Mail Ballots Before Election Day



Source: National Conference of State Legislatures.

most states allow election officials to preprocess mail ballots by verifying voters' identities, opening ballot envelopes, and scanning ballots into tabulators so that absentee ballot results can be obtained as soon as polls close. But some states — Alabama, Mississippi, New Hampshire, South Carolina, South Dakota, West Virginia, and the key battlegrounds of Pennsylvania and Wisconsin — do not allow any preprocessing of mail ballots before Election Day (see figure 1).[22] Those states should act to allow and encourage election officials to preprocess mail ballots ahead of Election Day.[23] And even states that allow some preprocessing before Election Day should increase the time period permitted. For example, while the Michigan legislature last year authorized election officials to preprocess mail ballots two days ahead of Election Day for some elections, the secretary of state and many election officials argued that a period of seven days is needed.[24]

For the 2023 legislative session, West Virginia and New Hampshire are each considering bills with provisions that would make it faster to count mail ballots.[25] The Maryland legislature, meanwhile, has passed a bill that will require mail ballot preprocessing to start ahead of Election Day.[26]

Build Resilience to False Election Claims

In the battle to stave off election disinformation, falsehoods have a particular edge: they swiftly emerge and proliferate, and there is inevitably a lag before officials can correct misperceptions. But recent studies offer insights into how to better combat election misinformation by building greater resilience ahead of time and, where possible, anticipating and preempting false narratives that will likely recur across different election contexts.

Indeed, election deniers rely on core deceptions that surface repeatedly.[27] Across major social media platforms during the 2022 midterms, these persistent tropes included stories assailing the integrity of mail ballots and voting machines, lies exploiting confusion about the vote counting timeline, and baseless accusations of noncitizens using names of the deceased to cast fraudulent ballots.[28] Additionally, when glitches occur on Election Day — typically innocuous mistakes that are quickly resolved — election deniers immediately spin stories that trade on these timeworn fabrications.[29]

The recurrent nature of deceptive election tropes means that election officials, public leaders, and civic organizations can prepare for the false claims that election deniers may make by educating voters to identify misinformation, providing facts to refute persistent falsehoods, and guiding the public toward reliable sources of information.

>> CISA and state and local election officials should develop and promote rumor control resources.

CISA's rumor control web page resource, Election Security Rumor vs. Reality, offers a good example of how officials can refute recurring election falsehoods by providing factual information geared toward the general public in a centralized location.[30] Many states — including Connecticut, Kentucky, and Ohio — have launched similar efforts, managing their own rumor control pages, hiring dedicated staff to organize and share factual information with voters, and publishing explainers that highlight the many steps election officials take to keep elections secure and accurate.[31]

Public officials at all levels must do more to expand these initiatives: CISA should augment its existing rumor control program by updating resources and ensuring broad dissemination, including to civil society organizations best equipped to amplify accurate information to groups targeted by disinformation campaigns. More states and local jurisdictions should also launch their own efforts with these same goals.

>> The EAC should undertake a broad communications effort to build public awareness and confidence in voting system security.

As previously discussed, spurious claims about the integrity of the nation's voting machines will likely be a core false narrative in the lead-up to the 2024 election. The EAC plays a crucial role in bolstering voting system security through its development and maintenance of the Voluntary Voting System Guidelines (VVSG), a national voting system testing and certification program that independently verifies voting system compliance with security, accessibility, and usability best practices.[32] As the EAC implements the latest version of the VVSG, adopted in 2021, the agency has produced essential guidance and resources to help election officials explain these new standards to voters and counter anticipated disinformation about the legal and practical implications of this transition.[33]

While the existing guidance and resources are an excellent step, the EAC should also work closely with CISA to proactively rebut election falsehoods by launching a broad communications and outreach effort to raise public awareness of the VVSG, how these standards protect election security, and what additional steps states can and will take to protect voting systems. As an independent, bipartisan federal agency with voting system expertise, the EAC is uniquely well-suited to push back on disinformation and build stronger public confidence in these systems.

In addition to creating templates and resources for election officials to adopt, the EAC should do more to reach the communities where deceptive rumors are likely to gain traction. Such efforts should include strengthening

connections with government agencies, nonprofits, community organizations, and other entities that are positioned to reach various segments of the American public and preparing tailored resources and information that these groups can convey to their audiences.

>> States should conduct targeted voter education and outreach efforts to preempt false election information.

As part of outreach efforts to curb election falsehoods, election officials and government agencies should educate voters about the timeline for counting votes and certifying election results. They should also explain existing security safeguards that preserve the integrity of voting, the vote-by-mail process, and vote counting machines. In past election cycles, various election offices have created videos to clarify how mail ballots are processed and counted, posted Election Day infographics to social media to explain the expected timeline for election results, and invited the public to participate in supervised tests of voting machines.[34] State legislatures should devote adequate funding to election offices for voter education and outreach efforts that help mitigate the spread of false election claims.

>> CISA should encourage public-private partnerships and share best practices with a wider network to build societal and institutional resilience to online disinformation.

Disinformation campaigns are likely to become increasingly sophisticated, persuasive, and widespread with continuing advances in AI and other emerging technologies. Beyond trying to get ahead of specific false claims, steps must be taken to build resilience to disinformation by improving digital and information literacy and increasing public understanding of election security. There is near universal agreement among election officials about how important this work is: in a 2023 Brennan Center for Justice Survey of local election officials, 85 percent stated that they believe it is beneficial for CISA to dispel falsehoods about elections by promoting accurate information about election administration and technology.[35] Building resilience to election disinformation also helps protect against foreign adversaries that seek to exploit election denialism to their own advantages. CISA and the executive branch as a whole must expand their roles in guarding against election falsehoods.

CISA should implement many of the suggestions that its Cybersecurity Advisory Committee (CSAC), an independent body that provides strategic recommendations to the agency's director, called for in its 2022 report "Protecting Critical Infrastructure from Misinformation and Disinformation."[36] In particular, CISA should

- build societal resilience to mis- and disinformation through broad public awareness campaigns, heightened information literacy, and civics education;
- convene government agencies, social media platforms, traditional media, researchers, businesses, faith and community organizations, and election officials to plan for expected threats during the 2024 election cycle;[37] and
- promote information from firsthand sources of facts, such as election officials and .gov election office websites.

Over the last few years, CISA has created or facilitated the creation of numerous publications intended to build societal resistance to disinformation and assist state and local jurisdictions to prepare for, identify, and combat disinformation. One example is its Tactics of Disinformation series, which provides real-world examples of disinformation campaigns by foreign governments as well as actions that state and local governments can take to limit the effects of similar campaigns. CISA has also encouraged parallel efforts through a working group led by state and local election officials alongside representatives from federal agencies, law enforcement, and election security industry partners. The group has supplied multilingual and accessible media resources to help election officials prepare for and respond effectively to falsehoods "that may impact the ability to conduct elections."[38]

CISA must continue to grow this work. The agency and the working group should expand the reach of their public-private partnerships, remaining closely connected and responsive to the current needs of stakeholders at the local and state levels. CISA and the working group should also continue to expand the existing mis-, dis-, and malinformation resource library with updated, multilingual, and multimedia resources and information on best practices to help election officials boost digital literacy around existing election security safeguards, improve access to accurate election information in their communities, and combat election falsehoods.[39] The agency should also provide election offices with resources to address the proliferation of rumors due to rapidly advancing generative AI capabilities.

Finally, CISA should expand its efforts to include broader networks to prepare for and build resilience to false election narratives ahead of the 2024 election. Specifically, CISA should enlist

- governmental associations such as the EAC, the National Association of Counties, the National Conference of State Legislatures, the National Governors Association, the National League of Cities, and the U.S. Conference of Mayors;
- chambers of commerce and other business associations; and

- community-based organizations, "especially organizations in specifically targeted communities, including veterans, faith communities, the Black and Latino communities, [and] immigrant communities," as CSAC recommends.[40]

These networks will help build institutional resilience to disinformation campaigns and bolster the dissemination of accurate election information to all voters.

II. Protect Election Workers

The people who run U.S. elections have become a target for those seeking to undermine American democracy.[41] The 2023 Brennan Center survey found that nearly one in three local election officials had faced harassment, abuse, or threats, and almost half were concerned about their colleagues' safety in future elections.[42] During the 2022 midterms, an election official in Arizona was forced into hiding for fear of his safety. And in 2023, authorities arrested a losing candidate in New Mexico in connection with shootings at the homes of elected officials whom he had previously approached with false allegations of election fraud.[43]

This disturbing trend is taking a toll on election officials, and many have left their jobs as a result. Indeed, 12 percent of election officials who responded to the survey began their positions after the 2020 election, and 11 percent say they are unlikely to continue to serve in the 2024 presidential election.[44] The loss of institutional knowledge that accompanies this turnover can lead to more administrative mistakes, which in turn fuel further conspiracy theories, distrust in the electoral process, and threats — or worse — against election workers.

The vicious cycle must be stopped. Although the United States avoided widespread violence in 2022, the 2024 election will bring more division and heightened tensions. More sophisticated and easily accessible AI tools could result in a rise of deepfakes — manipulated images, video, and audio used to misrepresent election officials and exacerbate threats against them. Now is the time to take action to protect election workers — and, ultimately, the electoral process.

Among other things, the federal government and the states must equip election officials with the resources they need to protect themselves and their staffs by providing additional funding opportunities and better communication as to how to access such funds. State lawmakers must also protect election workers proactively through greater privacy safeguards and updated laws that guarantee adequate protections not just at the polling place but in other locations where they are increasingly threatened, including at ballot tabulation centers and at home. Finally, federal, state, and local law enforcement must work together with election officials to ensure accountability for those who carry out attacks on democracy.

Increase Federal Support to Election Officials

The Russian cyberattacks in 2016 were met with a massive, coordinated federal response. DHS began by designating election systems as critical infrastructure. CISA followed by augmenting agency capabilities and establishing consistent, regular communication and information sharing with election officials. U.S. election infrastructure has faced unprecedented pressures and skepticism in the years since, but the system has been resilient in large part because of these federal efforts.

As threats have expanded from infrastructure to election workers, however, the federal government has failed to respond with the same level of investment or coordination. And election officials have noticed: in the Brennan Center's survey, nearly three in four election officials said that the federal government is either doing nothing to support them or not doing enough.[45] These agencies and departments must be proactive to protect election workers and demonstrate to the people running elections that the federal government has their back.

>> CISA should increase physical security guidance and resources for election workers and utilize regional election leads to coordinate outreach to election officials.

Amid heightened international and domestic conflict and ahead of a likely contentious presidential race in 2024, CISA must expand its work with local election offices over the next 18 months, and it must be given the resources it needs to do so. In the Brennan Center's Survey, only 31 percent of local election officials said that they were aware of CISA's physical security assessments, and just 20 percent of those who were aware availed themselves of this free service.[46]

CISA should increase the number of protective security advisers (PSAs) — experts in critical infrastructure who are trusted partners of government officials — available to assist local election offices with physical security assessments (and, as discussed in the next section of this report, offer insider threat guidance). The agency should also establish regional election leads to coordinate PSA outreach to election officials.

CISA should also release an election security strategic plan ahead of 2024, as it did before the 2020 election.[47] Such a plan is an opportunity to highlight physical security guidance and outreach along with other election

security priorities. Releasing and publicly promoting a strategic plan will help public officials and civil society understand what the most pressing challenges are, where to deploy resources, and what gaps need to be filled in the run-up to the presidential election.

>> DOJ should expand engagement with local election officials and law enforcement and reduce barriers to reporting threats.

In 2021, DOJ announced an election threats task force "to address the rise in threats against election workers, administrators, officials, and others associated with the electoral process."[48] In the years since, the task force has made only limited progress. Some critics point to the limited number of prosecutions since the task force launched: as of August 2022, DOJ had only charged eight cases out of more than a thousand reported threats, and only one had led to a conviction.[49] But frustration has also stemmed from a lack of information sharing between the federal effort and local officials — including both election officials, who are unsure how to report threats or whom to report them to, and local law enforcement, who receive incident reports from election officials but lack the resources and national context available at the federal level. The Brennan Center's survey found that 83 percent of local election officials have a specific point of contact with local law enforcement compared to just 5 percent who have a point of contact with federal law enforcement, and that election officials who faced threats were seven times more likely to report those threats to local law enforcement than they were to federal law enforcement.[50]

DOJ can take several steps to improve coordination and information sharing with these groups. First, the election threats task force should develop stronger partnerships, both formal and informal, with law enforcement at the local and state levels. DOJ could expand the task force through an enhanced collaborative model or by forming an advisory board of representatives from local and state law enforcement.

DOJ should also hire a senior adviser who has existing relationships with election officials to support and expand the department's outreach capacity. When CISA made a similar hire following the 2017 designation of election systems as critical infrastructure, the agency greatly improved both trust and collaboration with state and local election offices.[51] The Brennan Center's survey suggests that a DOJ hire could have the same impact — 89 percent of election officials said that hiring a staff member with experience and connections in the election community would increase their willingness to work with and trust DOJ.[52] The department has recently taken what may be a positive step in this direction, posting for a new "election community liaison position," but it remains to be seen who will be hired for this position and whether their previous work will garner the election community's trust.[53]

Finally, DOJ should reduce barriers for election officials to report threats or harassment. Enabling individuals making reports on the FBI's website to simultaneously upload supporting materials, including pictures, audio recordings, and screenshots of threatening messages, is one way to do so. DOJ representatives should also encourage greater reporting in public messaging with election officials by highlighting how reports — even those that do not result in charges being filed — are used in investigations, tracked, and included in systems for future investigative work.

Provide Funding for Physical Security

When conspiracy-driven protesters showed up to election offices in the aftermath of the 2020 election, they brought more than signs, megaphones, and cameras. Many carried guns. Armed individuals showed up in front of vote counting locations in Arizona, Michigan, Nevada, and Pennsylvania.[54] Guns also feature prominently in the threats that election officials receive: in Oregon, an election official looked down from her office to see the words "Vote don't work. Next time bullets." painted in large white letters in the parking lot below.[55]

State and local election officials need funding to bolster physical security at their offices and, when necessary, their homes. The needed security improvements — which include door locks, bulletproof doors and windows, panic alarm systems, key card access controls, exterior and parking lot lighting, security gates and fencing, communications systems, personal security training, and personal information protection services — would come at a significant cost: as much as $300 million nationally.[56] While some election offices have been able to upgrade their security, many more under-resourced offices have been unable to address even the most basic physical security vulnerabilities. Among the 54 local election officials interviewed by the Brennan Center who had received a CISA physical security assessment, insufficient funding was by far the number one reason cited for not implementing all the recommended improvements.[57]

>> DHS, DOJ, CISA, and the EAC should promote federal grant opportunities and help direct available funding to the areas of greatest need.

Existing federal grant programs can provide funding for physical security. DHS recently announced that state recipients of Homeland Security Grant Program (HSGP) funding will be required to spend at least 3 percent of received grants on election security needs in 2023 and to consult with their chief state election officials on how the funds should be used.[58] This change will result in around

$30 million in new funding for election security, including physical security improvements to protect election workers. DOJ also announced in 2022 that funds from the Edward Byrne Memorial Justice Assistance Grant (JAG) program could be used to protect election workers. However, to date, very little of this funding has made its way to election offices.[59]

Federal agencies and departments should increase outreach to state and local election officials to spread awareness of all federal funding opportunities that can be used to improve election workers' safety and security. CISA is particularly well-suited to coordinate and conduct this outreach, because of the relationships and trust the agency has built in the election community and its cyber and physical security expertise. CISA should develop a comprehensive communications plan for new regional election leads with the goal of proactively promoting federal funding opportunities and offering guidance on the most effective uses for available funding. Through EI-ISAC, CISA should also raise awareness of the new HSGP election security requirement, as well as SLCGP funding opportunities. And it should continue outreach and briefings on spending requirements with election officials and state administrative agencies that plan grant spending.

In addition, DOJ should urge state administrative agencies that plan JAG grant spending to prioritize election security needs and promote funding availability. The EAC can also play a role in educating election officials about the full suite of federal resources available to them.

>> State and local officials should make more funding available for physical security needs.

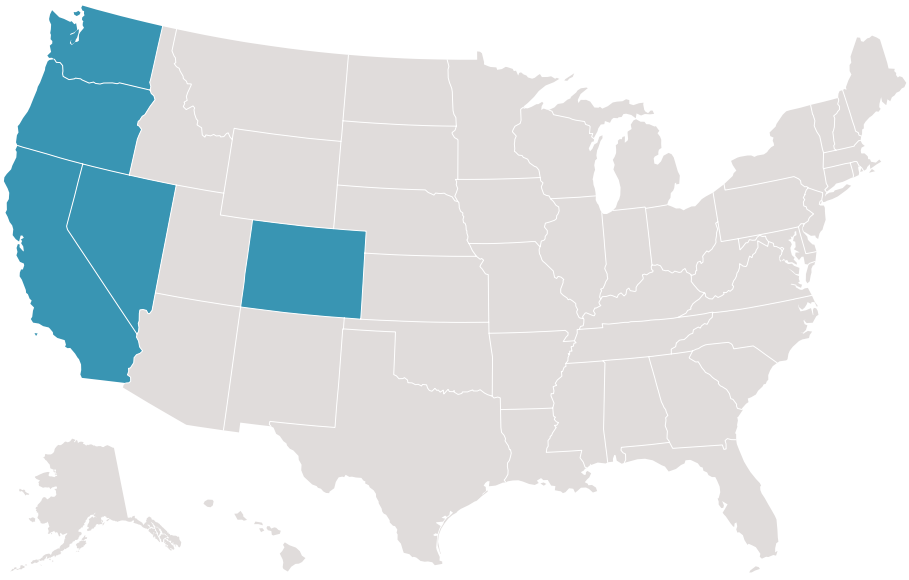
Federal grant funding alone will not be enough to address the physical security challenge. Yet despite the threats facing election officials and the rapid turnover of elections staff, few states have dedicated new funding to help election officials better protect themselves, their staffs, and their voters. State and local officials must direct funding toward augmenting the security of election offices, polling places, and counting facilities.

Protect Personally Identifiable Information

Threats to election officials and workers have not been contained to their offices; election officials have also been harassed and intimidated at their homes. Their parents, children, and other loved ones have been targeted as well.[60] Following the 2020 election, dozens of armed individuals stood outside Michigan Secretary of State Jocelyn Benson's home "shouting obscenities and chanting into bullhorns" as she was decorating her house for Christmas with her four-year-old child.[61] An election official in Milwaukee received a letter at her home calling her "a traitorous c***," prompting her to leave the state with her children for 10 days.[62] Many more officials have had their home addresses and phone numbers shared on the internet.[63]

FIGURE 2

States That Have Passed Laws Since 2020 to Help Election Workers Protect Personal Information



Source: Cal. S.B. 1131 (2022); Colo. H.B. 22-1273 (2022); Nev. A.B. 321 (2022); Or. H.B. 4144 (2022); and Wash. S.B. 5628 (2022).

While election officials hold public-facing positions and must be accessible to their communities, this cannot mean that they forfeit all personal safety and security or the safety of their loved ones. Election workers need reasonable protections to keep their personal information private and help them feel safer in their jobs. In the wake of Congress's recent failure to act on proposed protections, states must lead the way.[64]

>> State legislatures should pass laws that allow election workers to protect their personal information.

In 2022, several states passed laws that make it easier for election officials to keep their home addresses private (see figure 2). Oregon enacted legislation that allows election officials to have their addresses exempted from disclosure by county clerks as public records.[65] Colorado passed a bill allowing election officials at the state, county, and local levels to file a request with a government entity to remove personal information from online records.[66] California and Washington opened their address confidentiality programs to election workers who are targeted with threats or harassment.[67] Nevada allowed election officials to request a court order requiring their personal information to be kept confidential.[68] All states should implement similar protections.

Address confidentiality programs, which many states have already established, present an existing solution. These programs can offer substitute addresses to qualifying election workers who fear for their safety or the safety of their families, mitigating the risk that hostile individuals will target their homes or use their personal information to threaten them. State legislatures should pass laws that specifically permit election workers to qualify for these programs.

>> State officials should make address confidentiality programs more accessible to election workers.

In some states, election workers who have faced threats or fear for their safety may already be eligible for existing address confidentiality programs, even without legislative changes. In these cases, the official who oversees the address confidentiality program — often the secretary of state or attorney general — should conduct outreach and issue guidance to make it easier for election workers to avail themselves of such programs' benefits. These officials should take the following steps:

- Clarify that election workers do not have to move from their current residence to qualify for the program's benefits, as guidance for some address confidentiality programs currently asserts. Although these requirements may make sense for certain applicants who are survivors of domestic violence or stalking, they create unnecessary hurdles when the risk of harm does not stem from a single identifiable person. Election workers can still benefit from having their addresses less visible in public sources even if they remain at their current addresses.

- Train local election officials on how to assist workers in their offices with applications for address confidentiality programs.

- Assure that election workers need only assert in good faith that they meet the qualification standards for the program, such as being a target of ongoing threats or having a reasonable fear for safety, as applicable to the state's statute.

>> State legislatures should fund training and services to help election workers better protect their personal information online.

While laws extending personal information protection to election workers are much needed, they are not sufficient. States should supplement these protections with funding for personal information protection and online safety training. Such training could cover how election workers can avoid revealing their and their families' personal information or location, including turning off location tags in social media posts, asking websites to remove personal information, and avoiding posts that might inadvertently reveal locations of schools and homes. Grant funding could also pay for services from outside providers that help scrub personally identifying information for officials, conduct monthly checks to prevent information from becoming public again, and offer tailored guidance on how to protect personal information in the future.

Update Laws on Threatening and Doxing Election Workers

Although some states have advanced bills that would add new criminal penalties for threatening election workers, federal and state laws already on the books would cover most violent threats. Yet perpetrators have largely avoided accountability because too often these laws have not been enforced or incidents have not been fully investigated under the statutes. Federal, state, and local law enforcement must take these threats against election officials seriously and improve systems for reporting and investigating improper conduct.

State legislatures can encourage a more robust response by making sure that these existing laws reflect changing election systems and clarifying that intimidating an election worker because of their job is not protected speech.

>> State legislatures should ensure that laws that prohibit threatening election workers apply to all election workers throughout the entire election process.

As voting options have expanded in recent decades, election workers now serve in a broader variety of roles and interact with the public during a longer period — not just at polling places on Election Day but also at election offices, early voting locations, ballot drop boxes, and canvassing facilities. And individuals who seek to disrupt elections do so not just through intimidation at polling places but more generally with threats against those who administer elections wherever they are, before, during, and after Election Day.

States should ensure that existing laws prohibiting threats, harassment, and intimidation apply to all election workers performing election administration responsibilities, regardless of where the incident occurs. New Mexico recently expanded a law that previously only covered intimidation of poll workers, voters, and poll watchers to also include the secretary of state, county or municipal clerks, and any employees of these offices.[69] A bill in Virginia would amend a law that currently only covers threats at polling places to cover all threats against election workers intended to prevent them from administering elections.[70]

>> State legislatures should pass laws that prohibit doxing election workers.

States should also update or pass laws to prohibit doxing of election workers — the publication of an election worker's personal information with the intent to threaten their safety or with knowledge that the information will be used to facilitate threats against them. Colorado passed a bill in 2022 making it illegal for someone to intentionally share personal information about an election official or their immediate family on the internet if the sharing of that information creates an immediate and serious threat to their safety and the person sharing the information knows or should know about that danger.[71] Maryland is considering a bill with similar language.[72] A bill introduced in Oklahoma would add election officials to an existing anti-doxing statute that already covers state government officials.[73]

Such bills help to establish accountability for threats in which an election worker's personal address, telephone number, or other information is shared alongside direct calls for violence, putting their and their families' safety at risk.

>> State legislatures should provide state attorneys general and election workers with tools to bring civil actions against those making illegal threats.

Civil actions are a potential pathway to enforce prohibitions on threatening or intimidating election workers. State attorneys general and affected election workers themselves should be allowed to seek civil relief against someone making illegal threats, including by seeking a restraining order to prevent ongoing harm.

The federal Voting Rights Act offers a model for this kind of law. It prohibits individuals from intimidating or threatening any person for "voting or attempting to vote" or "for urging or aiding any person to vote or attempt to vote."[74] If an individual violates this prohibition, or if there is reason to believe that someone is going to violate this provision, federal law authorizes the U.S. attorney general and other covered persons to sue in court for a temporary or permanent injunction, restraining order, or other equitable relief to prevent ongoing harm.

States should enact similar provisions to protect election workers. In doing so, state legislatures should expressly state that the law prohibits intimidation or threats against all election workers performing election administration duties.

III. Defend Against Insider Threats

Almost one-third of Americans still believe the false narrative that Joe Biden won the 2020 presidential election due to fraud.[75] Unsurprisingly, some of the more than 8,000 local election officials — along with tens of thousands of public- and private-sector employees who support their work — also buy into this conspiracy theory. Even on a very small scale, the endorsement of election misinformation by individuals charged with administering elections is a particularly dangerous threat to democracy.

Throughout and since the 2020 election, election officials and workers who support election falsehoods have attempted to use their access to voting systems or positions of power in a manner that undermines election security. These insider threats include sharing access to critical election systems with election deniers, spreading false information about the security of elections and election equipment, attempting to replace voting systems with less accurate and less secure methods for counting ballots, and refusing to perform mandated responsibilities, such as certifying election results.

In 2022, election deniers running for office in battleground secretary of state contests were roundly rejected. But in other states, election deniers won those races.[76] And across the country, many more won contests or were appointed at the local level, where ballots are counted and election operations are run.[77] As election deniers continue to influence or replace election workers, the risk of insider threats will grow.

Accordingly, officials at all levels of government must blunt efforts to improperly access or misuse critical election infrastructure. They must also implement policies that make it more difficult for a rogue election administrator or worker to disrupt processes in a way that confuses or delays certification of accurate election results.

Set Access Restrictions

Since 2020, there have been at least 17 reported incidents in which election deniers have gained or attempted to gain access to voting systems, often in coordination with an election official or worker.[78]

In one such occurrence, a county clerk in Colorado with connections to prominent election conspiracy theorists gave unauthorized individuals access to the county's voting system, allowing them to copy the hard drives of the voting equipment.[79] The information obtained was later shared online, resulting in a state investigation, which found that the county clerk had given an unauthorized person a key card and turned off video surveillance of the voting machines.[80]

To prepare for similar future attempts, states must have protocols in place not only to prevent unauthorized access to critical election systems but also to detect and respond to such access if these preventive measures fail.

>> State legislatures should pass laws to limit access to election infrastructure and ensure that election offices can catch any unauthorized actions.

State legislators should set broad, baseline requirements for election system access in state law, including rules for monitoring and storing voting machines, which have been the most frequent target of election deniers. Following the breach in Colorado, the state legislature passed a law requiring election offices to keep all voting systems in a location monitored by 24/7 video surveillance and secured by a key card access system that logs the name, date, and time of each entrance.[81]

When determining the baseline requirements to set in statute, state legislatures must avoid standards that are so rigid that they cannot be updated as technology and security concerns evolve. Rather than dictating specific technology or security systems, legislation should focus on the outcome of such protections — for example, by requiring local election offices to have a system that can keep unauthorized individuals out of voting system storage and automatically produce a log of all entrances rather than mandating a particular system that would accomplish this task.

To ensure conformance with the latest cyber and physical security best practices, state legislatures should direct the chief state election official to issue and regularly update more detailed regulations and guidance on voting system access. States can also include this direction within a broader mandate that the chief election official produce a complete, enforceable election procedures manual. Legislators in Nevada have introduced a bill that would require the secretary of state to produce such a guide.[82]

>> State legislatures should prohibit tampering with or facilitating unauthorized access to voting equipment.

State legislators should pass laws that prohibit anyone from tampering with voting equipment, accessing such

equipment without authorization, or facilitating access for an individual who is not an authorized election worker or voting system vendor. Lawmakers in Kansas and Minnesota introduced bills with such provisions in 2023, and Colorado passed a similar prohibition in 2022.[83] These bills also contain specific prohibitions on publicly sharing passwords for voting systems and imaging hard drives of voting equipment.

Such laws should include exceptions to allow for legitimate security research. For instance, a chief state election official should be able to approve one-time access to an outside researcher on request by a local election official. State law should specify exemption conditions that protect the security of equipment, such as requiring the researcher to complete a background check. When the chief state election official approves a request, the law should require the office to publish the approval, along with the reason for granting access and any conditions tied to it.

>> State and local election officials should develop detailed standards to regulate who can access election infrastructure and how that access can occur.

State and local election officials should exercise their regulatory and guidance authority to set standards that will help prevent, detect, and respond to insider threats. The specifics of these standards may vary depending on the systems in use and the size and structure of election offices throughout the state. The following is a list of standards that states have set to safeguard election systems:

- Requiring election offices to keep all voting system components and ballots in a secure location with access controls, alarm systems, and procedures to log every entry.[84]
- Monitoring voting equipment storage areas with video surveillance.[85]
- Requiring all election workers and voting system vendors to complete background checks before allowing access to voting systems.[86]
- Requiring two employees to be present whenever voting equipment is accessed or transported, and at least one election worker to be present with voting system vendors while the vendor is on-site.[87]
- Requiring that election offices create an individual user account for each person who is authorized to access election systems and prohibiting users from sharing account or password information.[88]
- Limiting election system access privileges to election officials and workers whose responsibilities require access to these systems, only permitting access to the extent necessary for the performance of these job functions, and capping the number of user accounts that jurisdictions can offer access privileges to without state approval.[89]
- Requiring all users with access to election systems to sign an acceptable use policy agreement provided by the state.[90]
- Disabling election system access accounts immediately for users who are no longer employed by the election office or who are no longer in roles that require access to that system.[91]

In developing access restrictions, election officials must balance security with appropriate flexibility to make sure that limited authorization does not slow operations or prevent election offices from responding to emergencies or other issues that necessitate a rapid response.

To ensure accountability when handling sensitive systems and materials, state and local election officials should also add requirements for bipartisan or two-person teams to perform vital election administration responsibilities where possible.

>> State and local legislatures should fund infrastructure to prevent insider threats.

A 2022 Brennan Center analysis found that upgrades to protect against insider threats could cost up to $316 million nationwide.[92] State and local legislators should provide funding for election officials to purchase the systems and equipment necessary to comply with any new state requirements and more generally to safeguard against insider threat risks.[93] In Colorado, when the state legislature passed its recent bill to protect against insider threats, it established a $1 million grant fund to assist counties in complying with the new security requirements, including to purchase key card access systems and video surveillance.[94] Other states should follow that lead.

States should also look to federal grants to help fund these improvements, including DHS's HSGP and SLCGP.

Improve Training and Guidance

As local election offices across the country experience turnover, some states, including Colorado and Nevada, have considered or passed bills to expand training and certification requirements for election officials.[95]

Comprehensive training does more than just ensure that election officials are aware of and prepared to implement all protocols needed to keep election infrastructure secure; it also facilitates relationships and information sharing between newer and more experienced election officials.

>> State legislatures should mandate regular, comprehensive training for all election officials.

State law should require, at a minimum, all local election officials to attend biennial training on election administration procedures. New local election officials should be required to attend training before administering any state or federal election, if possible. Municipal clerks in Minnesota who have taken office less than six months before an election must complete two hours of emergency training from their home county auditor or secretary of state before administering the election.[96] State legislatures could also designate — or allow the chief state election official to designate — additional individuals who must attend training, including state election office employees and other local election workers who have access to critical election systems.

State lawmakers can also prevent election officials who do not complete training requirements from accessing critical election systems or from performing certain responsibilities. A recent law in Colorado established the role of "designated election official" — the official or employee in each county who oversees access to election systems — and prohibits individuals from performing this role unless they have been certified as having completed training requirements.[97]

State legislators should provide funding to reimburse local election officials for the cost of attending training.

>> CISA should develop additional insider threat best practices and self-assessment tools and train protective security advisers to offer insider threat mitigation guidance.

In 2022, CISA released an "Election Infrastructure Insider Threat Mitigation Guide," which advised election officials on how to respond to the rising risk of insider threats by adopting standard operating procedures, access controls, zero-trust security, and chain-of-custody measures.[98] Ahead of the 2024 presidential election, CISA should expand its insider threat services by creating additional best practice checklists, using them to develop self-assessment tools for officials, and training PSAs on these materials and practices so that they can offer insider threat guidance to election officials around the country. In developing these additional resources, CISA should consult with other federal partners, including the Federal Emergency Management Agency (FEMA), the Office of the Director of National Intelligence, and the National Insider Threat Task Force, each of which has its own expertise on this topic.[99]

Ideally, PSAs would provide hands-on guidance and scenario-based training on how to

- establish a formal insider threat program, including an organizational structure and confidential processes that are easy to understand and use;[100]
- identify and protect critical assets;
- recognize suspicious behavior and other threat indicators; and
- take appropriate actions to mitigate potential insider threats.[101]

Finally, CISA should utilize the local and state election official networks of the EI-ISAC, the National Association of Secretaries of State, the National Association of State Election Directors, and the Election Center (the National Association of Election Officials) to ensure that its resources on insider threats are reaching as wide an audience as possible.

>> DOJ should reissue guidance to remind election officials of requirements to preserve election records.

After public officials in Arizona and other states turned election records, materials, and equipment over to unqualified outside parties in 2021, DOJ issued guidance to election officials on their duty under federal law to safeguard and preserve federal records.[102] Ahead of the 2024 election, DOJ should issue a reminder of this duty and reiterate that the obligation to preserve records remains on election officials, even if they turn those materials and records over to a third party. Releasing and publicizing this guidance can support election officials looking to resist political interference and deter those who may be susceptible to outside pressure.

Establish Authority to Remediate Risks

State legislators must ensure that, if an insider threat does impact election systems, state officials can respond quickly and effectively to remediate any potential security risks that may affect an election.

>> State legislatures should establish clear authority to prohibit individuals who violate election laws from administering elections and to decommission equipment when a breach occurs.

State legislators should authorize state election officials to prevent any individual who has shown a serious or patterned failure to comply with security requirements found in state law from administering elections or from performing certain responsibilities such as accessing the voter registration system. The Colorado secretary of state successfully sued the county clerk who permitted unauthorized access to voting systems to prevent her from overseeing elections in 2022.[103] Similarly, the

Michigan secretary of state directed a township clerk to refrain from overseeing an election after the clerk refused to allow routine and required maintenance on voting equipment.[104]

CISA has noted that if critical systems have been compromised, "the safest practice is to decommission and replace those systems."[105] That being the case, state legislatures should also authorize state election officials to investigate any system or equipment breach and to decommission and order the removal and replacement of specific equipment if necessary. Since 2020, officials in Arizona, Colorado, Georgia, Michigan, and Pennsylvania have all acted to decommission election systems that were tampered with or accessed without proper authorization (see figure 3).[106]

While these remedies are necessary to address ongoing threats to election security, state legislatures must carefully define the authority to prevent abuse by future officials.

Use Voting Machines for Initial Ballot Counts and Pair with Robust Postelection Audits

Spurred by false information about the security and reliability of electronic voting machines, election deniers across the country have pushed election officials to abandon secure and proven technology for counting ballots and instead count all ballots solely by hand. Hand-counting procedures play an important role in verifying election outcomes through postelection audits that election officials conduct in addition to voting system tabulation. But such audits hand-count only a few races on a random sample of ballots after results produced by voting systems have already been collected and reported.

Counting every race on every ballot by hand to determine the initial vote count in anywhere but the smallest jurisdictions is impractical and often inaccurate. When election workers need to count every race on a large number of ballots, hand-counting consistently produces more errors than machine tabulation.[107] When a Nevada county attempted to conduct a hand-count during the 2022 election, the county clerk estimated that there was a 25 percent error rate among the election volunteers counting ballots in the first day.[108] Full hand-counts are also much slower than machine counts, leading to significant delays in producing election results, conducting necessary audits or recounts, resolving any election disputes, and finalizing election results.

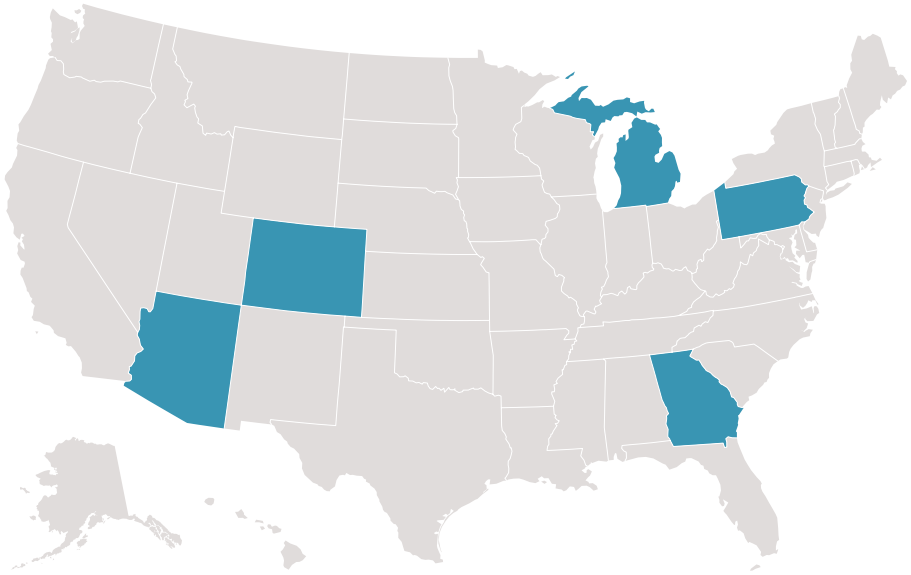
Left unchecked, hand-counting could lead to serious accuracy concerns, disinformation, and uncertainty in the days and weeks after Election Day.

>> State legislatures should require election officials to use machines for initial ballot counts in all but the smallest jurisdictions.

State legislators should require election officials to use voting tabulation systems for initial counts, with limited exceptions for very small jurisdictions. States should pair

FIGURE 3

States Where Officials Have Decommissioned Election Equipment Following a Physical Breach



Source: Brennan Center.

voting system counts with robust postelection audits, in which officials hand-count small samples of ballots to verify machine-tallied results.

Small jurisdictions with few registered voters may be able to produce a final count that is comparably accurate to what tabulation equipment would produce in a similar time frame. But these jurisdictions are very much the exception — most places that hand-count ballots today are small towns with fewer than 1,000 voters. Just 0.6 percent of all registered voters live in such jurisdictions.[109]

Make It More Difficult to Refuse to Certify Elections

Insider threat risks extend beyond access to systems. Election officials can also jeopardize election security and integrity by abusing their authority to oversee crucial steps in the election process, including the certification of election results.

>> State legislatures should create a mandatory duty to certify election results and a legal remedy to address refusals to do so.

Fortunately, in states where rogue officials have refused to certify election results, state leadership has been able to step in and quickly address the issue. In New Mexico, the secretary of state immediately sued and obtained a court order against a county that refused to certify primary election results in 2022, forcing the county to reverse course.[110] All states must ensure that they can act with similar speed if an issue arises in their own elections. Even if these abuses are unlikely to change election outcomes, delays in addressing the matter lend support to false election narratives and cast more doubt on election results.

Ahead of 2024, state legislatures should streamline processes in their statutory frameworks for election results certification to address refusals to certify elections. In particular, legislators should ensure that state law establishes

- a mandatory, nondiscretionary duty to certify election results by a stated deadline;
- a cause of action that a state official or candidate can bring in court against an official who refuses to certify election results without sufficient cause; and
- a remedy that allows a court to compel the official to certify results within a short time span.

IV. Ensure Technical Resilience

Compared to 2016, the U.S. election system today is far more resilient to attacks.[111] This strengthened position is due to public officials' contributions at every level: state and local election officials adopted cybersecurity best practices in their daily operations; federal, state, and local officials improved resource and information sharing; and Congress provided meaningful federal funding in 2018 and 2019 to help states upgrade election systems and safeguard against cyberattacks. The 2020 election was called the "most secure in American history" because of these combined efforts.[112]

But cybersecurity is a race without a finish line. Even with substantial investment leading up to the 2020 presidential election, 31 states today will be using voting equipment for the 2024 election that is at least a decade old (see figure 4).[113] These outdated machines are not only more vulnerable than machines manufactured to the latest security standards but also far more likely to cause problems on Election Day.[114] At the same time, election offices are seeing high staff turnover and risk losing the considerable institutional knowledge that has helped election workers more effectively mitigate and respond to vulnerabilities.

Cybersecurity pressures have not subsided. Foreign adversaries continue to meddle in U.S. elections, including during the 2022 midterms.[115] The United States cannot afford to lose ground and let election systems slip back into a vulnerable position.

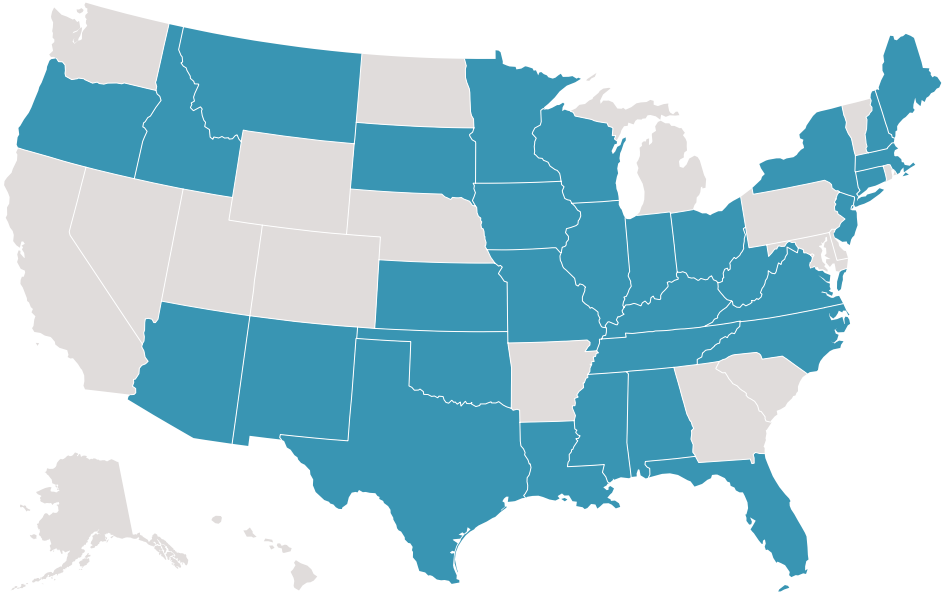
Federal, state, and local governments must invest in election infrastructure by providing adequate resources to replace and upgrade outdated systems and to defend those systems. Election officials must meanwhile put in place protections to prevent and recover from any cyberattacks or equipment failures. They should do so by developing contingency plans around things that may go wrong during the voting period and by implementing robust postelection audits to confirm election outcomes.

Fund the Replacement of Outdated Infrastructure

One of the most important election security measures is the use of paper ballots. When voters record selections on paper, they can easily verify that their ballots accurately reflect their choices. Election officials can also check paper ballots against electronic vote totals after

FIGURE 4

States Using Principal Voting Equipment That Will Be at Least 10 Years Old in 2024



Source: Brennan Center analysis of Verified Voting data, as of April 7, 2023.

an election to confirm that voting machines are working as intended.

>> State legislatures should require voting systems with paper records and fund the transition to and upkeep of this equipment.

Since 2016, states have made significant progress in adopting paper ballots. In 2020, an estimated 93 percent of all votes cast in the presidential election had a paper record — up from 82 percent four years earlier.[116]

Many states that use paperless voting systems are aiming to replace these systems in the coming years. Since 2020, Indiana, Mississippi, Tennessee, and Texas have all either passed laws requiring voting systems to produce a paper record of every vote or moved up the deadline for doing so.[117] But these transitions will only be realized if election officials have the resources needed to purchase new equipment that complies with these laws. New Jersey serves as a cautionary tale: state law has required paper voting systems for more than a decade, but counties remain out of compliance with the law in part due to inadequate funding for upgrades.[118]

In the 2024 election, 100 percent of all votes can and should be cast on paper.

Still, even paper-based voting systems risk becoming less secure and less reliable as the equipment ages and maintenance becomes more difficult and costly. State legislators must provide sufficient funding to upgrade equipment and outfit election systems with the latest security protections.

>> Congress should provide steady funding to help election officials upgrade and maintain election infrastructure.

Election offices need reliable and meaningful federal funding for substantial technological investments and for the upkeep that those systems will require in years to come. After providing $805 million in election security funding leading up to the 2020 election, Congress has since provided just $150 million in irregular bouts of funding.[119] States need more and consistent funding to upgrade voting machines and registration systems, hire additional cybersecurity support, and implement thorough postelection audits.[120]

Plan for Things That Can Go Wrong

Online voter registration has made it easier for eligible voters to add their names to the voter rolls and for election officials to keep voter rolls up-to-date.[121] Electronic pollbooks have expedited check-in processes and shortened lines at polling places.[122] And electronic tabulators have led to more accurate and timely vote counts.[123] Election officials can and should use all of this technology in the election process, but increased technological dependence requires careful planning to guarantee election resilience.

>> State and local election officials should improve measures to recover from technical failures and resource shortages.

Election officials must ensure that they have measures in place to prevent and recover from cyberattacks, technical failures, and resource shortages so that no error or mishap will prevent a voter from casting their ballot or having their vote counted.[124] Election offices should conduct comprehensive reviews of their election processes and develop contingency plans for any potential technical failure on Election Day. Should an issue arise, officials should ensure that they have enough backup materials to keep polling places operational for the two to three busiest hours of the day, buying time until the issue can be resolved.

States should adopt the following resilience measures:

- Requiring polling places to have a paper backup list of voters or a voter list on a nonnetworked alternative device in case of electronic pollbook failure.
- Requiring polling places to have an adequate supply of provisional ballots and envelopes in case of errors in the registration database.
- Requiring polling places to have emergency paper ballots that can be hand-marked and cast into a scanner or stored to be centrally counted later in case of ballot marking device or direct recording electronic voting machine failure.

Many states have codified expanded voting options that became popular during the pandemic.[125] As states continue to make voting more accessible to more voters, election officials should ensure that existing resilience measures are still adequate. If a state uses vote centers and networked electronic pollbooks for early or Election Day voting, a nonnetworked alternative device may be better equipped than a paper backup to hold a larger voter list and more easily update inoperative electronic pollbooks once they are working again. If a state offers active same-day voting registration or adopts early voting yet has insufficient time to reallocate ballots to Election Day poll sites, jurisdictions may need to print more than enough ballots for all registered voters heading into the voting period.

>> State and local election officials should develop resources to help implement contingency plans and communicate these measures to the public.

Resilience measures are effective only if the relevant workers know how to implement them when needed.

State and local election officials should incorporate contingency plans into poll worker training and create short, easy-to-locate, and easy-to-follow guides for poll workers to turn to if needed on Election Day. Election officials should also consider how to communicate backup measures to voters and reassure them that their votes will still be counted. Officials should prepare explainer videos, signs, and other materials in advance for contingency plans that are regularly relied on, such as the use of emergency auxiliary bins on scanners.

Conduct Robust Postelection Audits

The security benefits of paper ballots are fully realized only when election officials routinely review the independent paper record to confirm that the voting system determined the correct outcome. Most states now require election officials to conduct postelection audits, which typically involve hand-counting a portion of the paper records and comparing them to the electronic counts produced by voting machines after scanning the same ballots.[126] The most common form of postelection audit is a traditional audit, in which election officials count a fixed percentage of all ballots cast in each election. States that use traditional postelection audits could improve their procedures to better assure voters that their ballots have been counted correctly.

>> States should adopt and implement risk-limiting audits.

A risk-limiting audit (RLA) operates similarly to a traditional postelection audit, in that both require election workers to hand-count a sample of ballots and compare the results to the machine count. But a traditional postelection audit provides confirmation that individual voting machines are accurately tabulating votes, whereas an RLA relies on statistical principles to determine the random sample of ballots that needs to be counted and provides evidence that election outcomes are accurate, including for statewide races.

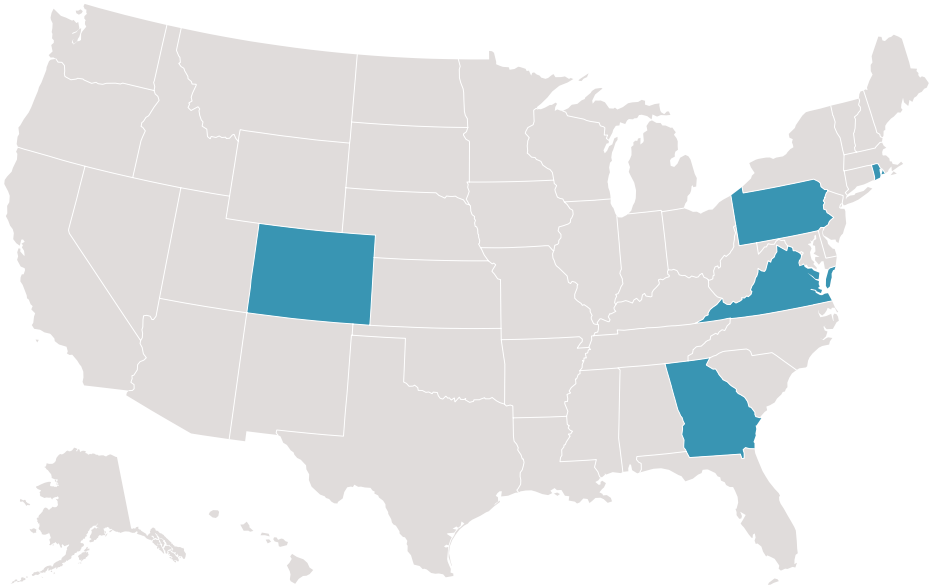
States should require RLAs after every election, following an appropriate transition period for election officials to learn proper procedures and ensure that they have the systems in place to carry out the process. Five states currently require RLAs (see figure 5). Where RLAs are not obligatory, state and local election officials should consider piloting RLAs as state law permits, in addition to any required postelection audits.

Increase Support for Under-resourced Local Election Offices

In the decentralized U.S. election system, "target rich, resource poor" local jurisdictions with limited capacity to address cybersecurity issues present one of the most

FIGURE 5

States That Require Risk-Limiting Audits



Source: Data from Verified Voting, as of April 7, 2023.

concerning vulnerabilities.[127] These election offices have little or no dedicated cybersecurity expertise and are often dependent on other offices in their county or municipality for IT support. In fact, nearly half of all election offices operate with one or fewer full-time employees, and nearly a third operate with no full-time staff at all.[128] Yet election officials who serve these offices are given the monumental task of being frontline national security figures. They need help.

>> State legislatures should provide funding to launch cyber navigator programs.

States should hire cyber navigators — trained cybersecurity and election administration professionals who work closely with local election officials to assess the security of their systems, identify potential vulnerabilities, and develop tailored strategies to mitigate risk. Several states, including Florida, Illinois, Iowa, Massachusetts, Michigan, Minnesota, and Ohio, have deployed cyber navigator programs already.[129] Other states should follow suit.

>> DHS, CISA, and FEMA should elevate cybersecurity funding opportunities for election security and prioritize outreach to election officials.

Existing federal grant programs can improve the cybersecurity capacity of local election offices; the new SLCGP alone will provide $1 billion for cybersecurity needs over the next four years.[130] As with HSGP grants, DHS should require states to spend a portion of SLCGP funding on election cybersecurity needs and consult with chief state election officials on election security priorities. CISA and FEMA should also promote federal funding opportunities to state and local officials, raise awareness of the HSGP minimum spending requirement, and encourage spending on election security needs.

Finally, CISA should direct PSAs and cybersecurity advisers (CSAs) — trained cybersecurity experts who can assist state and local officials — to prioritize outreach to under-resourced local election offices and use regional election leads to coordinate outreach with these officials. In the Brennan Center's 2023 survey, only 29 percent of local election officials said that they were aware of CISA's cybersecurity vulnerability scan, and just 20 percent of those who were aware availed themselves of this free service.[131]

Conclusion

The evolving threats to American democracy over the last decade have resulted in massive changes to the way elections are seen as well as the way they are administered. Although the last few years in particular have witnessed successful efforts to make the system more resilient, more needs to be done.

For the most part, the American public did its part in 2022, soundly rejecting election deniers who sought influence over elections in crucial battleground states like Arizona, Georgia, Michigan, Nevada, and Pennsylvania. Elected leaders and public officials at the federal, state, and local levels must act with similar urgency ahead of 2024.

Substantial work needs to be done to protect the people, systems, and infrastructure necessary for voters to cast their ballots and have their votes counted. But there is still time. Past success in strengthening U.S. infrastructure against cyberattacks and the renewed call by voters to defend democracy should give every American the hope and expectation that their leaders will rise to the challenge.

Endnotes

1 DHS, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

2 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, February 6, 2023, 15, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

3 Isabelle Niu, Kassie Bracken, and Alexandra Eaton, "Russia Created an Election Disinformation Playbook. Here's How Americans Evolved It," *New York Times*, October 25, 2020, https://www.nytimes.com/2020/10/25/video/russia-us-election-disinformation.html; and National Intelligence Council, *Foreign Threats to the 2020 US Federal Elections*, March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

4 Ellen Nakashima, Amy Gardner, and Aaron C. Davis, "FBI Links Iran to Online Hit List Targeting Top Officials Who've Refuted Trump's Election Fraud Claims," *Washington Post,* December 22, 2020, https://www.washingtonpost.com/national-security/iran-election-fraud-violence/2020/12/22/4a28e9ba-44a8-11eb-a277-49a6d1f9dff1_story.html.

5 Matt Vasilogambros, "Russian Cyberattack Could Capitalize on Election Doubts," Pew Charitable Trusts, April 22, 2022, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/04/22/russian-cyberattack-could-capitalize-on-election-doubts.

6 Sophia Tulip, "Iranian 'Hacking' Video Fabricated to Push Election Disinfo," Associated Press, November 7, 2022, https://apnews.com/article/fact-check-2020-election-fake-hacking-video-034512361997.

7 National Intelligence Council, *Foreign Threats to the 2020 US Federal Elections*.

8 Jennifer Agiesta, "CNN Poll: Americans' Confidence in Elections Has Faded Since January 6," CNN, July 21, 2022, https://www.cnn.com/2022/07/21/politics/cnn-poll-elections/index.html; and Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey," March 10, 2022, https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey-march-2022.

9 Ian Vandewalker, *Digital Disinformation and Vote Suppression*, Brennan Center for Justice, September 2, 2020, https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression; and Common Cause and Lawyers' Committee for Civil Rights Under Law, *Deceptive Election Practices and Voter Intimidation: The Need for Voter Protection*, July 2012, 4, https://lawyerscommittee.org/wp-content/uploads/2015/07/DeceptivePracticesReportJuly2012FINALpdf.pdf.

10 Maya Kornberg, Mekela Panditharatne, and Ruby Edlin, "3 Lessons on Misinformation in the Midterms Spread on Social Media," Brennan Center for Justice, January 5, 2023, https://www.brennancenter.org/our-work/research-reports/3-lessons-misinformation-midterms-spread-social-media; and William T. Adler, "Only 1 in 4 Election Websites Uses the .gov Domain. That's a Problem — and an Opportunity," Center for Democracy and Technology, October 19, 2022, https://cdt.org/insights/only-1-in-4-election-websites-uses-the-gov-domain-thats-a-problem-and-an-opportunity.

11 Jana Winter, "DHS Warns of Fake Election Websites Potentially Tied to Criminals, Foreign Actors," Yahoo News, August 21, 2020, https://www.yahoo.com/video/exclusive-dhs-warns-of-fake-election-websites-potentially-tied-to-criminals-foreign-actors-221029900.html.

12 FBI and CISA, "Foreign Actors Likely to Use Information Manipulation Tactics for 2022 Midterm Elections," public service announcement, October 6, 2022, https://www.cisa.gov/sites/default/files/publications/PSA-information-activities_508.pdf.

13 CISA, "Sign Up for a .gov Domain: Information for Election Officials," accessed March 31, 2023, https://www.cisa.gov/sites/default/files/publications/DOTGOV_Domain_Fact-Sheet_508_0.pdf.

14 Adler, "Only 1 in 4 Election Websites Uses the .gov Domain."

15 Frank LaRose (Ohio secretary of state) to Ohio State county boards of elections, June 11, 2019, https://www.ohiosos.gov/globalassets/elections/directives/2019/dir2019-08.pdf.

16 CISA, "Registration," accessed March 31, 2023, https://get.gov/registration.

17 DHS, "The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2022 State and Local Cybersecurity Grant Program," September 16, 2022, https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2022-state-and-local; and Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 429 (2021), https://www.congress.gov/bill/117th-congress/house-bill/3684/text.

18 Common Cause and Lawyers' Committee for Civil Rights Under Law, *Deceptive Election Practices and Voter Intimidation*.

19 Kan. Admin. Regs. § 25-2415 (2012), https://www.ksrevisor.org/statutes/chapters/ch25/025_024_0015.html; Minn. R. 204C.035 (2022), https://www.revisor.mn.gov/statutes/cite/204C.035; and 313 Va. Admin. Code. § 24.2-1005.1 (2007), https://law.lis.virginia.gov/vacode/title24.2/chapter10/section24.2-1005.1.

20 Miss. H.B. 678 (2023), http://billstatus.ls.state.ms.us/2023/pdf/history/HB/HB0678.xml#codesections; Minn. H.F. 3 (2023), https://www.revisor.mn.gov/bills/bill.php?f=HF3&b=house&y=2023&ssn=0; N.Y. S.B. 263 (2023), https://www.nysenate.gov/legislation/bills/2023/S263; and Anna Gustafson, "Benson, Dem Lawmakers Announce Plans to Protect Election Officials in Wake of Threats," *Michigan Advance*, January 18, 2023, https://michiganadvance.com/2023/01/18/benson-dem-lawmakers-announce-plans-to-protect-election-officials-in-wake-of-threats.

21 Mekela Panditharatne et al., *Information Gaps and Misinformation in the 2022 Elections*, Brennan Center for Justice and First Draft News, August 2, 2022, https://www.brennancenter.org/our-work/research-reports/information-gaps-and-misinformation-2022-elections.

22 National Conference of State Legislatures, "Table 16: When Absentee/Mail Ballot Processing and Counting Can Begin," last updated January 18, 2023, https://www.ncsl.org/elections-and-campaigns/table-16-when-absentee-mail-ballot-processing-and-counting-can-begin#toggleContent-12088.

23 National Conference of State Legislatures, "Table 16: When Absentee/Mail Ballot Processing and Counting Can Begin"; Mich. H.B. 4491 (2022), http://www.legislature.mi.gov/(S(b3osed3e3ezcmoorv3o44fw2))/mileg.aspx?page=GetObject&objectname=2021-HB-4491; and Karina Elwood, "Maryland Judge Allows Early Mail-Vote Counting to Avoid Result Delays," *Washington Post*, September 23, 2022, https://www.washingtonpost.com/dc-md-va/2022/09/23/maryland-mail-voting-judge-decision.

24 Clara Hendrickson, "Whitmer Signs Election Law Changes Including Ballot Preprocessing," *Detroit Free Press*, October 7, 2022, https://www.freep.com/story/news/politics/elections/2022/10/07/whitmer-signs-ballot-preprocessing-bill/69534507007.

25 W. Va. S.B. 156 (2023), http://www.wvlegislature.gov/Bill_Text_HTML/2023_SESSIONS/RS/bills/sb156%20intr.pdf; and N.H. H.B. 484 (2023), https://www.gencourt.state.nh.us/bill_status/billinfo.aspx?id=360&inflect=2.

26 Md. H.B. 0535, https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb0535?ys=2023RS; and Md. S.B. 0379,

https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0379?ys=2023RS.

27 Renée DiResta, "Arizona's 'Tricky Voting Machines' Sounds Suspiciously Familiar," *Atlantic*, November 12, 2022, https://www.theatlantic.com/ideas/archive/2022/11/arizona-election-voting-machines-fraud-conspiracy-tv-tropes/672100.

28 Kornberg, Panditharatne, and Edlin, "3 Lessons on Misinformation."

29 Panditharatne et al., *Information Gaps*.

30 CISA, "Election Security Rumor vs. Reality," accessed March 31, 2023, https://www.cisa.gov/rumorcontrol.

31 Cecilia Kang, "Help Wanted: State Misinformation Sheriff," *New York Times*, May 31, 2022, https://www.nytimes.com/2022/05/31/technology/misinformation-sheriff-election-midterms.html; Office of the Kentucky Secretary of State, "Rumor Control," last updated November 5, 2021, https://sos.ky.gov/elections/Pages/Rumor-Control.aspx; and Ohio Secretary of State, "Sec LaRose: The Life of an Absentee Ballot," YouTube, October 23, 2020, https://www.youtube.com/watch?v=n4Vz3r8QC6k&t=2s.

32 Election Assistance Commission, "Voluntary Voting System Guidelines," accessed March 30, 2023, https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines.

33 Election Assistance Commission, "Voluntary Voting System Guidelines (VVSG) Deprecation," accessed March 30, 2023, https://www.eac.gov/election-officials/voluntary-voting-system-guidelines-vvsg-deprecation#Resources.

34 Ohio Secretary of State, "Sec LaRose: The Life of an Absentee Ballot"; Michigan Department of State (@MichSoS), "In election administration, accuracy and security are more important than speed. Every valid vote will be counted," Twitter, November 8, 2022, https://twitter.com/MichSoS/status/1590143800860889088?s=20&t=KbcknsdKCZhEArhpdMm5Pg; and Adriana De Alba and Ariel Plasencia, "Tarrant, Dallas Counties to Let the Public Test Its Voting Machines in a Push to Boost Confidence in Elections," WFAA (ABC 8 Dallas), September 22, 2022, https://www.wfaa.com/article/news/politics/tarrant-county-letting-public-test-voting-machines-in-push-to-boost-confidence-elections/287-781010ab-b7a4-40dc-92a5-266d0b451507.

35 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023," April 25, 2023, https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey-april-2023.

36 CSAC, "Report to the CISA Director: Protecting Critical Infrastructure from Misinformation and Disinformation" June 22, 2022, https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20%E2%80%93%20MDM_0.pdf.

37 CSAC, "Report to the CISA Director."

38 See CISA, "Rumor Control Page Start-Up Guide," accessed March 30, 2023, https://www.cisa.gov/sites/default/files/publications/rumor-control-startup-guide_508.pdf; and CISA, "Mis-, Dis-, and Malinformation: Planning and Incident Response Guide for Election Officials," accessed March 31, 2023, https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf.

39 CISA, "MDM Resource Library," accessed March 30, 2023, https://www.cisa.gov/mdm-resource-library.

40 CSAC, "Report to the CISA Director," 4.

41 Brennan Center for Justice and Bipartisan Policy Center, *Election Officials Under Attack*, June 16, 2021, https://www.brennancenter.org/our-work/policy-solutions/election-officials-under-attack.

42 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023."

43 Kate Sullivan and Kyung Lah, "Maricopa County Election Officials Moved to Undisclosed Location on Election Day Due to Threats," CNN, November 22, 2022, https://www.cnn.com/2022/11/21/politics/maricopa-bill-gates-threat-undisclosed-location/index.html; and Remy Tumin and Mike Ives, "Republican Ex-candidate Arrested in Shootings Targeting New Mexico Democrats," *New York Times*, January 16, 2023, https://www.nytimes.com/2023/01/16/us/albuquerque-democrat-officials-shootings-arrest.html.

44 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023."

45 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023."

46 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023."

47 CISA, "#Protect2020 Strategic Plan," February 2020, https://www.cisa.gov/sites/default/files/publications/ESI_Strategic_Plan_FINAL_2-7-20_508.pdf.

48 DOJ, "Justice Department Launches Task Force to Combat Threats Against Election Workers," July 29, 2021, https://www.justice.gov/opa/blog/justice-department-launches-task-force-combat-threats-against-election-workers-0.

49 Kate Holland et al., "Facing Threats of Violence, Election Officials Are Growing Frustrated with DOJ Task Force," ABC News, November 2, 2022, https://abcnews.go.com/US/facing-threats-violence-election-officials-growing-frustrated-doj/story?id=92495137.

50 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023."

51 Lawrence Norden et al., "How Federal Departments and Agencies Can Help Secure America's Elections," Brennan Center for Justice, April 21, 2022, https://www.brennancenter.org/our-work/research-reports/how-federal-departments-and-agencies-can-help-secure-americas-elections.

52 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023."

53 DOJ, "Trial Attorney (Election Community Liaison)," job posting, USAJOBS, March 9, 2023, https://www.usajobs.gov/job/711699000.

54 Tim Sullivan and Adam Geller, "Increasingly Normal: Guns Seen Outside Vote-Counting Centers," Associated Press, November 7, 2020, https://apnews.com/article/protests-vote-count-safety-concerns-653dc8f0787c9258524078548d518992.

55 Matt Vasilogambros, "States Want to Boost Protections for Threatened Local Election Officials," Pew Charitable Trusts, March 9, 2022, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/03/09/states-want-to-boost-protections-for-threatened-local-election-officials.

56 Derek Tisler and Lawrence Norden, "Estimated Costs for Protecting Election Workers from Threats of Physical Violence," Brennan Center for Justice, May 3, 2022, https://www.brennancenter.org/our-work/research-reports/estimated-costs-protecting-election-workers-threats-physical-violence.

57 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023."

58 DHS, "DHS Announces $2 Billion in Preparedness Grants," press release, February 27, 2023, https://www.dhs.gov/news/2023/02/27/dhs-announces-2-billion-preparedness-grants.

59 Sean Lyngaas, "'Our Security Here Is a Joke': Election Workers Lament Lack of Federal Spending on Security Ahead of Crucial Midterms," CNN, October 27, 2022, https://www.cnn.com/2022/10/27/politics/election-security-federal-funding-violent-threats/index.html.

60 Linda So and Jason Szep, "U.S. Election Workers Get Little Help from Law Enforcement as Terror Threats Mount," Reuters, September 8, 2021, https://www.reuters.com/investigates/special-report/usa-election-threats-law-enforcement.

61 Office of the Secretary of State Jocelyn Benson, "Statement from Secretary of State Jocelyn Benson Concerning Threats Against Her and Her Family," December 6, 2020, https://www.michigan.gov/sos/0,4670,7-127-93094-546741--,00.html.

62 Adam Brewster, "Key Local Election Officials in Battleground States Still Face Threats over a Year After 2020 Election," CBS News, January 4, 2022, https://www.cbsnews.com/news/election-officials-threats-2020-election.

63 Brennan Center and Bipartisan Policy Center, *Election Officials Under Attack*.

64 Enhanced Election Security and Protection Act, S. 4574, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/4574/text.

65 Or. H.B. 4144 (2022), https://olis.oregonlegislature.gov/liz/2022R1/Measures/Overview/HB4144.

66 Colo. H.B. 22-1273 (2022), https://leg.colorado.gov/sites/default/files/2022a_1273_signed.pdf.

67 Cal. S.B. 1131 (2022), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB1131; and Wash. S.B. 5628 (2022), https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Session%20Laws/Senate/5628-S.SL.pdf?q=20230323184416.

68 Nev. A.B. 321 (2021), https://www.leg.state.nv.us/App/NELIS/REL/81st2021/Bill/7842/Text.

69 N.M. S.B. 43 (2023), https://nmlegis.gov/Sessions/23%20Regular/bills/senate/SB0043.pdf.

70 Va. S.B. 907 (2023), https://lis.virginia.gov/cgi-bin/legp604.exe?231+ful+SB907S1+pdf.

71 Colo. H.B. 22-1273 (2022).

72 Md. H.B. 0951 (2023), https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0951?ys=2023RS.

73 Okla. S.B. 481 (2023), http://www.oklegislature.gov/BillInfo.aspx?Bill=sb481&Session=2300.

74 52 U.S.C. § 10307(b).

75 Mark Murray, "Poll: 61% of Republicans Still Believe Biden Didn't Win Fair and Square in 2020," NBC News, September 27, 2022, https://www.nbcnews.com/meet-the-press/meetthepressblog/poll-61-republicans-still-believe-biden-didnt-win-fair-square-2020-rcna49630.

76 Lawrence Norden and Marina Pino, "Election Deniers Running for Secretary of State Were This Election's Biggest Losers," Brennan Center for Justice, November 11, 2022, https://www.brennancenter.org/our-work/analysis-opinion/election-deniers-running-secretary-state-were-elections-biggest-losers; and Adrian Blanco, Daniel Wolfe, and Amy Gardner, "Tracking Which 2020 Election Deniers Are Winning, Losing in the Midterms," *Washington Post*, December 18, 2022, https://www.washingtonpost.com/politics/interactive/2022/election-deniers-midterms.

77 Nicholas Riccardi, "'Election Denial Is Alive and Well': Despite Statewide Losses, Conspiracists Win Some Local Offices," *Los Angeles Times*, November 19, 2022, https://www.latimes.com/world-nation/story/2022-11-19/election-conspiracists-claim-some-races-for-local-offices.

78 Nathan Layne and Peter Eisler, "Michigan Widens Probe into Voting System Breaches by Trump Allies," Reuters, June 7, 2022, https://www.reuters.com/world/us/exclusive-michigan-widens-probe-into-voting-system-breaches-by-trump-allies-2022-06-06.

79 Bente Birkeland, "After Data Is Posted on Conspiracy Site, Colorado County's Voting Machines Are Banned," NPR, August 12, 2021, https://www.npr.org/2021/08/12/1027225157/after-data-is-posted-on-conspiracy-website-colo-countys-voting-machines-are-bann.

80 Emma Brown, "An Elections Supervisor Embraced Conspiracy Theories. Officials Say She Has Become an Insider Threat," *Washington Post*, September 26, 2021, https://www.washingtonpost.com/investigations/an-elections-supervisor-embraced-conspiracy-theories-officials-say-she-has-become-an-insider-threat/2021/09/26/ee60812e-1a17-11ec-a99a-5fea2b2da34b_story.html.

81 Colo. S.B. 22-153, § 13 (2022), https://leg.colorado.gov/sites/default/files/documents/2022A/bills/sl/2022a_sl_322.pdf.

82 Nev. S.B. 54, § 2 (2023), https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/9608/Overview.

83 Kans. H.B. 2086 (2023), http://www.kslegislature.org/li/b2023_24/measures/hb2086/; Minn. H.F. 635 (2023), https://www.revisor.mn.gov/bills/bill.php?b=House&f=HF0635&ssn=0&y=2023; and Colo. S.B. 153 (2022), https://leg.colorado.gov/bills/sb22-153.

84 See, e.g., Ariz. Elec. Code Ch. 4, § III(A) (2019), https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf#page=109; Ga. Comp. R. and Regs. 183-1-12-.04(3) (2023), https://rules.sos.state.ga.us/gac/183-1-12; N.M. Code R. § 1.10.34.8(A) (2023), https://www.srca.nm.gov/parts/title01/01.010.0034.html; and Ohio Election Official Manual, Ch. 2, § 1.07 (2019), https://www.ohiosos.gov/globalassets/elections/directives/2019/dir2019-11_eom.pdf#%5B%7B%22num%22%3A260%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C70%2C680%2C0%5D.

85 See, e.g., N.M. Code R. § 1.10.34.8(B) (2023).

86 See, e.g., Colo. Code Regs. § 11.1.1 (2022), https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule11.pdf.

87 See, e.g., Ariz. Elec. Code Ch. 4, §§ III(A)(7), III(B) (2019); and Colo. Code Regs. §§ 20.5.4, 20.8.2(e) (2022), https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule20.pdf.

88 See, e.g., Colo. Code Regs. § 20.9.1 (2022); N.M. Code R. § 1.10.35.11(A) (2023), https://www.srca.nm.gov/parts/title01/01.010.0035.pdf; and Ohio Election Official Manual, Ch. 2, § 1.07 (2019).

89 See, e.g., Colo. Code Regs. § 20.9.1 (2022); and Ohio Election Official Manual, Ch. 2, § 1.07 (2019).

90 See, e.g., Colo. Code Regs. § 20.9.1(b)(2) (2022).

91 See, e.g., Colo. Code Regs. § 20.9.1(a)(4) (2022); and N.M. Code R. § 1.10.35.11(B) (2023).

92 Lawrence Norden, Derek Tisler, and Turquoise Baker, "Estimated Costs for Protecting Election Infrastructure Against Insider Threats," Brennan Center for Justice, March 7, 2022, https://www.brennancenter.org/our-work/research-reports/estimated-costs-protecting-election-infrastructure-against-insider.

93 Norden, Tisler, and Baker, "Estimated Costs for Protecting Election Infrastructure."

94 Colo. S.B. 22-153 (2022).

95 Colo. S.B. 22-153 (2022); and Nev. S.B. 54, § 2 (2023).

96 Minn. R. 8240.2700(9), https://www.revisor.mn.gov/rules/8240.2700.

97 Colo. S.B. 22-153 (2022).

98 CISA, "Election Infrastructure Insider Threat Mitigation Guide," June 2022, https://www.cisa.gov/sites/default/files/publications/election_insider_threat_mitigation_guide_508_0.pdf.

99 Federal Emergency Management Agency, "IS-915: Protecting Critical Infrastructure Against Insider Threats Course," last updated July 10, 2013, https://training.fema.gov/is/courseoverview.aspx?code=IS-915&lang=en; National Counterintelligence and Security Center, "Establish an Insider Threat Program," Office of the Director of National Intelligence, accessed March 31, 2023, https://www.dni.gov/index.php/safeguarding-science/insider-risk; and National Counterintelligence and Security Center, "National Insider Threat Task Force (NITTF) Mission," Counterintelligence and Security Center, accessed March 31, 2023, https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf.

100 CISA, "Human Resources' Role in Preventing Insider Threats," accessed March 31, 2023, https://www.cisa.gov/sites/default/files/publications/HRs%20Role%20in%20Preventing%20Insider%20Threats%20Fact%20Sheet_508.pdf.

101 DHS, "Insider Threat Mitigation Program," fact sheet, accessed March 31, 2023, https://www.cisa.gov/sites/default/files/publications/fact-sheet-insider-threat-mitigation-program-092018-508.pdf; and CISA, *Insider Threat Mitigation Guide*, November 2020, https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.

102 DOJ, *Federal Law Constraints on Post-Election "Audits,"* July 28, 2021, https://www.justice.gov/opa/press-release/file/1417796/download.

103 Ernest Luning, "Tina Peters Barred from Overseeing This Year's Primary and General Elections in Mesa County," *Colorado Politics*, May 10, 2022, https://www.coloradopolitics.com/elections/2022/tina-peters-barred-from-overseeing-this-years-primary-and-general-elections-in-mesa-county/article_1e42b2e8-d0b8-11ec-94ab-2fe94e87ecc4.html.

104 Jonathan Brater (Michigan director of elections) to Stephanie Scott (Adams Township clerk), October 25, 2021, https://content.govdelivery.com/attachments/MISOS/2021/10/25/file_attachments/1976229/Letters%20to%20Adams%20Township%20Clerk.pdf.

105 Rosalind S. Helderman, "Arizona Secretary of State Says Maricopa County Should Replace Election Equipment Because GOP-Backed Recount Compromised Its Security," *Washington Post*, May 20, 2021, https://www.washingtonpost.com/politics/arizona-audit-voting-equipment/2021/05/20/a8370368-b9a4-11eb-a5fe-bb49dc89a248_story.html.

106 Lawrence Norden, "Brennan Center Letter to State Associations of Election Officials on Addressing Voting Equipment Breaches," Brennan Center for Justice, August 12, 2022, https://www.brennancenter.org/our-work/research-reports/brennan-center-letter-state-associations-election-officials-addressing; and Nicole Garcia, "Maricopa Count Tests New Voting Machines Following Election Audit," Fox 10 (Phoenix), October 18, 2021, https://www.fox10phoenix.com/news/maricopa-county-tests-new-voting-machines-following-election-audit.

107 Rachel Orey, Christopher Thomas, and Grace Gordon, "How Ballot Tabulators Improve Elections," Bipartisan Policy Center, April 25, 2022, https://bipartisanpolicy.org/explainer/how-ballot-tabulators-improve-elections; and Alice Clapman and Ben Goldstein, "Hand-Counting Votes: A Proven Bad Idea," Brennan Center for Justice, November 23, 2022, https://www.brennancenter.org/our-work/analysis-opinion/hand-counting-votes-proven-bad-idea.

108 Brett Forrest, "Nye County Clerk Tempers Hand Count Expectations, Calls It a 'Test,'" NBC 3 News (Las Vegas), November 12, 2022, https://news3lv.com/news/local/nye-county-clerk-tempers-hand-count-expectations-calls-it-a-test.

109 Verified Voting, "Election Officials Need a Helping Hand, Not Hand Count Legislation," April 7, 2022, https://verifiedvoting.org/blog-hand-counts-4-7-22.

110 Alexandra Ulmer, "New Mexico Top Court Orders County to Certify Primary Results," Reuters, June 15, 2022, https://www.reuters.com/world/us/new-mexico-sues-county-over-refusal-certify-june-primary-results-2022-06-15.

111 Lawrence Norden and Derek Tisler, "The 2020 Election May Be the Most Secure in U.S. History," *Foreign Affairs*, October 15, 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-15/2020-election-may-be-most-secure-us-history.

112 CISA, "Joint Statement from Elections Infrastructure Government Coordinating Council and the Election Infrastructure Sector Coordinating Executive Committees," press release, November 12, 2020, https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

113 Turquoise Baker et al., "Voting Machines at Risk in 2022," Brennan Center for Justice, March 1, 2022, https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-2022.

114 Pam Fessler, "Report: America's Aging Voting Machines Could Present Election Problems," NPR, September 15, 2015, https://www.npr.org/sections/itsallpolitics/2015/09/15/440255752/report-americas-aging-voting-machines-could-present-election-problems.

115 Ines Kagubare, "Cyber Command Chief: Election Interference Is Not Going Away," *Hill*, March 3, 2023, https://thehill.com/policy/cybersecurity/3888331-chinese-cyberspace-threats-are-growing; and A. J. Vicens, "Foreign Disinformation Efforts to Interfere in US Midterms Mostly Fizzle, but Remain Concerning, Researchers Say," CyberScoop, December 19, 2022, https://www.cyberscoop.com/2022-midterm-election-interference-nation-state.

116 Derek Tisler and Turquoise Baker, "Paper Ballots Helped Secure the 2020 Election — What Will 2022 Look Like?," Brennan Center for Justice, May 10, 2022, https://www.brennancenter.org/our-work/analysis-opinion/paper-ballots-helped-secure-2020-election-what-will-2022-look.

117 Ind. H.B. 1116 (2022), https://iga.in.gov/legislative/2022/bills/house/1116; Miss. S.B. 2879 (2022), http://billstatus.ls.state.ms.us/2022/pdf/history/SB/SB2879.xml; Tenn. S.B. 2558 (2022), https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB2558&GA=112; and Tex. S.B. 598 (2021), https://capitol.texas.gov/BillLookup/History.aspx?LegSess=87R&Bill=SB598.

118 Nikita Biryukov, "Bill Would Revive Stalled Rule Requiring State's Voting Machines Leave Paper Trail," *New Jersey Monitor*, February 16, 2022, https://newjerseymonitor.com/briefs/bill-would-revive-stalled-rule-requiring-states-voting-machines-leave-paper-trail.

119 U.S. Election Assistance Commission, "Election Security Grant," accessed March 31, 2023, https://www.eac.gov/payments-and-grants/election-security-funds.

120 Lawrence Norden and Edgardo Cortés, "What Does Election Security Cost?," Brennan Center for Justice, August 15, 2019, https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost.

121 Brennan Center for Justice, *The Case for Voter Registration Modernization*, January 2, 2013, https://www.brennancenter.org/sites/default/files/publications/Case%20Voter%20Registration%20Modernization.pdf.

122 Emma Jones, "Smart Use of Electronic Poll Books Can Reduce Long Lines on Election Day," Bipartisan Policy Center, July 1, 2020, https://bipartisanpolicy.org/blog/smart-use-of-electronic-poll-books-can-reduce-long-lines-on-election-day.

123 Orey, Thomas, and Gordon, "How Ballot Tabulators Improve Elections."

124 Edgardo Cortés et al., *Preparing for Cyberattacks and Technical Problems During the Pandemic: A Guide for Election Officials*, Brennan Center for Justice, June 5, 2020, https://www.brennancenter.org/our-work/research-reports/preparing-cyberattacks-and-technical-problems-during-pandemic-guide.

125 Elise Viebeck, "States Across the Country Are Dropping Barriers to Voting, Widening a Stark Geographic Divide in Ballot Access," *Washington Post*, June 23, 2021, https://www.washingtonpost.com/politics/voting-rights-expansion-states/2021/06/22/1699a6b0-cf87-11eb-8014-2f3926ca24d9_story.html; and Zach Montellaro, "The Pandemic Changed How We Vote. These States Are Making the Changes Permanent," *Politico*, June 22, 2021, https://www.politico.com/news/2021/06/22/pandemic-voting-changes-495411.

126 National Conference of State Legislatures, *Post-Election Audits*, last updated September 22, 2022, https://www.ncsl.org/elections-and-campaigns/post-election-audits.

127 CISA, "CISA Establishes Ransomware Vulnerability Warning Pilot Program," press release, March 13, 2023, https://www.cisa.gov/news-events/news/cisa-establishes-ransomware-vulnerability-warning-pilot-program.

128 Paul Gronke and Paul Manson, "The State of Election Administration in 2022," Democracy Fund, November 2, 2022, https://democracyfund.org/idea/the-state-of-election-administration-in-2022.

129 Matt Vasilogambros, "Facing Foreign Election Foes, States Hire 'Cyber Navigators,'" Pew Charitable Trusts, August 25, 2021, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/08/25/facing-foreign-election-foes-states-hire-cyber-navigators.

130 "State and Local Cybersecurity Grant Program," last updated November 3, 2022, https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program.

131 Brennan Center for Justice and Benenson Strategy Group, "Local Election Officials Survey — April 2023."

ABOUT THE AUTHORS

▶ **Derek Tisler** is counsel in the Brennan Center's Elections and Government Program. His work focuses on issues related to election administration, security, and disinformation. He is a coauthor of several recent Brennan Center reports, including *Election Officials Under Attack (2021), Ensuring Safe Elections* (2020), and *A Roadmap to the Official Count in an Unprecedented Election* (2020). His work has been featured in media outlets across the country, including *Foreign Affairs*, *FiveThirtyEight*, and the *Hill*. Tisler has received a BA in economics from Michigan State University and his JD from the University of Chicago Law School.

▶ **Lawrence Norden** is senior director of the Brennan Center's Elections and Government Program. He has authored several nationally recognized reports and articles related to election administration and voting technology, including *Securing Elections from Foreign Interference* (2017), *America's Voting Machines at Risk* (2015), *How to Fix Long Lines* (2013), *Better Design, Better Elections* (2012), and *Voting Law Changes in 2012* (2011). His work has been featured in media outlets across the country, including the *New York Times*, the *Wall Street Journal*, CNN, Fox News, MSNBC, and NPR. He has testified before Congress and several state legislatures on numerous occasions. He received his JD from NYU School of Law.

ABOUT THE BRENNAN CENTER'S DEMOCRACY PROGRAM

The Brennan Center's Democracy Program encourages broad citizen participation by promoting voting and campaign finance reform. We work to secure fair courts and to advance a First Amendment jurisprudence that puts the rights of citizens — not special interests — at the center of our democracy. We collaborate with grassroots groups, advocacy organizations, and government officials to eliminate the obstacles to an effective democracy.

ACKNOWLEDGMENTS

The Brennan Center gratefully acknowledges The William and Flora Hewlett Foundation, Carnegie Corporation of New York, Change Happens Foundation, FJC - A Foundation of Philanthropic Funds, Leon Levy Foundation, Zegar Family Foundation, Craig Newmark Philanthropies, Scarlet Feather Fund, and Jerome L. Greene Foundation for their generous support of our work. This is an independent Brennan Center publication; the opinions expressed are those of the authors and do not necessarily reflect the views of our supporters.

The authors would like to thank the many colleagues who contributed to this report. They would especially like to thank Mekela Panditharatne and Julia Fishman, who contributed crucial research, drafting, and editing support, as well as Kathy Boockvar, Alice Clapman, Lisa Danetz, Veronica Degraffenreid, Liz Howard, Lauren Miller, Sean Morales-Doyle, Marina Pino, and Gowri Ramachandran, who provided invaluable knowledge, insights, and guidance that informed this report's recommendations, and Ruby Edlin, who assisted with editing and fact-checking.

BRENNAN CENTER FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
www.brennancenter.org