POLICY SPOTLIGHT: FIVE APPROACHES TO ACTUALLY SECURE U.S. ELECTIONS

SEPTEMBER 2022

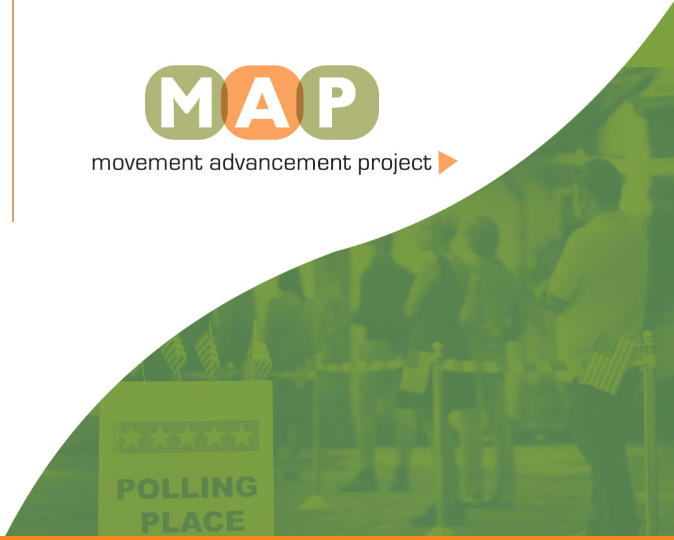
Introduction

A cornerstone of U.S. democracy is free and fair elections. Without voters knowing that their votes will be counted, that counts are accurate, and that there is no interference from external or internal forces, our democracy will crumble. Policies that work to secure our elections while also preserving access for voters include protecting election officials, preventing insider election threats, modernizing voter registration, securing in-person voting processes, and proper use of post-election audits.

Since the 2016 election, additional attention has been paid to election security. In 2016, a new threat to our democracy arose: foreign hacking and interference. During that cycle, at least 21 states were targeted by foreign hackers and at least one state's voter registration system was breached. In 2020, another threat to democracy emerged, this time from inside our country's borders. False allegations of voter fraud led to the insurrection on January 6th, the closest America has come to losing our democracy since the Civil War. Even now, as we look towards the 2022 elections, significant portions of the Republican party have adopted the election denialism mantle, and candidates for office across the country are winning primary elections on the same false platform while also claiming to want to advance policies to secure our elections.

Rather than advancing legislation based on false claims of voter fraud, states must adopt policies that will actually protect and secure our elections while maintaining access to the ballot for all eligible voters. Evidence is clear that the policies covered in this report, including protecting election officials, preventing insider threats, automatic voter registration, secure voting machines, and post-election audits, can all help to achieve these goals.

MAP
movement advancement project



Election Security Approach #1: Protecting Election Officials from Threats and Harassment

Threats to election officials have risen to unprecedented levels following the 2020 election, where false allegations of voter fraud and violent rhetoric led to the insurrection on January 6th. According to a recent survey by the Brennan Center, one in three election officials reported feeling unsafe because of their job, and one in five listed threats to their lives as a job-related concern. In recent hearings held by the U.S. Senate, a Justice Department official testified that the agency has reviewed more than 1,000 hostile threats directed at election officials just this year. In Georgia, employees in a county elections office endured months of death threats, resulting in at least one staff person going into hiding. In Pennsylvania, a Republican member of the Philadelphia election board faced a series of threats, including to his family. In Vermont, police investigated threats against employees in the Elections Division of the Secretary of State's office.

This alarming rise in violent threats has led to a mass exodus of qualified election officials. While the specific number of departures is not available in all states, the trend is clear: According to reporting by the Associated Press and the *New York Times*, at least 1/3 of Pennsylvania's county election officials have quit since November 2020. At least 1/4 of election directors in southwest Ohio have recently quit. Similar numbers of resignations have occurred in Kansas, Michigan and Wisconsin. In August, all three employees of the elections office in Gillespie County, Texas resigned due to threats and harassment, leaving the office unstaffed less than three months before Election Day. Such an exodus accelerates the dangerous trend of extreme partisan actors seeking to fill these roles and further emboldens those promoting false theories of election fraud. According to a recent analysis by CNN, in at least 10 states the Republican candidate running for the state's chief election office has espoused election conspiracy theories and/or advocated for overturning the results of the 2020 election.

Violent Threats to Election Workers

U.S. election workers get little help from law enforcement as terror threats mount

Read full Reuters article **here.**

I HOPE YOU ALL GO TO JAIL FOR TREASON. I HOPE YOUR CHILDREN GET MOLESTED. YOU'RE ALL GOING TO F——— DIE.

THREAT TO NEVADA ELECTION WORKERS

THIS IS WHAT YOU'RE GOING TO F——— GET FROM NOW ON. YOU'RE ALL GOING TO F——— DIE, AND IT IS WHAT YOU DESERVE.

THREAT TO NEVADA ELECTION WORKERS

WATCH YOUR BACK. I KNOW WHERE YOU SLEEP, I SEE YOU SLEEPING. BE AFRAID,

THREATENING FACEBOOK MESSAGE TO COLORADO SECRETARY OF STATE JENA GRISWOLD

COPS CAN'T HELP YOU. HEADS ON SPIKES.

ANONYMOUS THREAT SENT TO THE WIFE OF PHILADELPHIA CITY COMMISSIONER AL SCHMIDT

YOU'RE GOING TO BE SERVED LEAD.

ANONYMOUS THREATTO FULTON COUNTY, GEORGIA, ELECTIONS DIRECTOR RICHARD BARRON

The federal government, along with a small number of states, has taken action to protect these election officials. The Justice Department's newly established Election Threats Task Force has initiated at least five prosecutions so far this year. Federal law has stricter standards and penalties for prosecuting these kinds of threats, but some states have acted to strengthen their generally applicable laws to provide additional safeguards for election officials. As shown in **Figure 1**, only three states have enacted laws to create additional protections for election workers (Colorado, Oregon, and Maine).

In Colorado, Secretary of State Jena Griswold sponsored passage of the Election Official Protection Act, which increases protections in state law that currently prohibit interfering with an official's work by adding language making it a crime to threaten or intimidate an election official. A new law in Maine makes it a crime to intentionally interfere by any physical act with a person performing an official function relating to a federal, state or municipal election. And in Oregon, a law passed this year allows election workers to have their address exempted from disclosure as public record by county clerk and establishes that the crime of harassment includes harassment against an election worker.

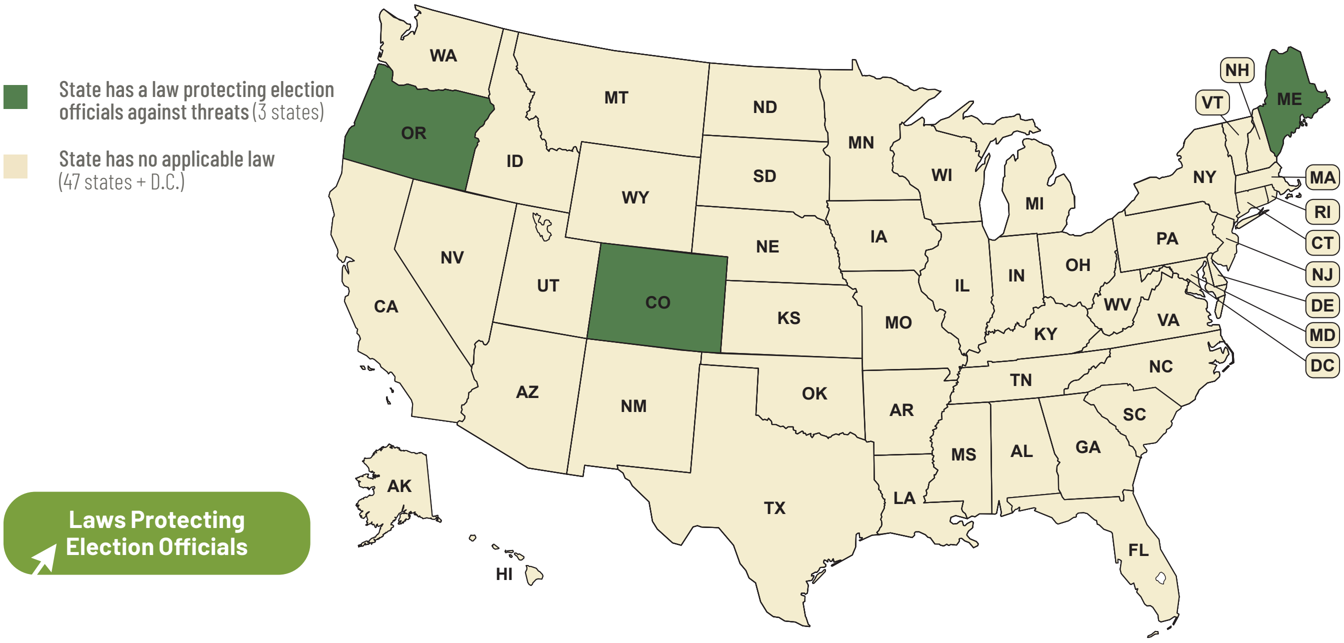
While this is a new and emerging area of state law, every legislature is capable of passing legislation as discussed above to protect our election officials and hold accountable the people who threaten them. The thousands of officials across the country who run our elections do not deserve to live in fear simply for doing their jobs. All levels of government can and should do more to protect these people who work so hard to protect and uphold our democracy.

Election Security Approach #2: Preventing Insider Threats

While the focus surrounding the 2016 election concerned foreign interference in our elections, following the 2020 election a new threat emerged: interference and sabotage by actors from the inside. The growing number of threats to election officials discussed in the prior section of this report, and the resulting mass exodus, has opened a gap that is increasingly being filled by election deniers and promoters of conspiracy theories.

The influx of these extreme partisan actors has led to serious election security breaches in at least five states. New reporting by the *Washington Post* suggests that a legal team working for former President Trump orchestrated a coordinated plan to breach

FIGURE 1: LAWS PROTECTING ELECTION OFFICIALS AGAINST THREATS



🟩 State has a law protecting election officials against threats (3 states)
State has no applicable law (47 states + D.C.)
WA
OR
ID
MT
ND
SD
WY
NV
CA
UT
CO
NE
KS
AZ
NM
OK
TX
MN
IA
MO
AR
LA
WI
IL
MI
IN
OH
KY
TN
MS
AL
GA
FL
SC
NC
VA
WV
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC
AK
HI
Laws Protecting Election Officials

voting systems in at least three states—Georgia, Nevada, and Michigan. Evidence has emerged that this team was dispatched to Coffee County, Georgia, on the day following the attack on the Capitol. The team was reportedly allowed to make copies of essentially every aspect of the county's election system—an unprecedented breach. Also notable is the case of Tina Peters, a county election clerk in Colorado, who is under indictment for her role in a scheme to copy hard drives containing confidential voting data in an attempt to validate false theories of election fraud. This breach later resulted in the data being published on third-party conspiracy websites. Despite being under indictment, Peters ran for the Republican nomination for Secretary of State, and following her recent primary loss continued to claim that voter fraud invalidated the results of her election—all while raising hundreds of thousands of dollars from private donors for a recount. In Michigan, investigations are ongoing in at least four jurisdictions regarding unauthorized access and security breaches of voting equipment; these investigations allegedly involve the same legal team of the former president involved in the breaches in Georgia discussed above. The Republican candidate for Attorney General in Michigan, Matt Deperno, is a subject of the investigation after he allegedly bragged about gaining access to voting equipment during a 2021 interview. In Pennsylvania, state officials were forced to decertify voting machines after a rural county gave third parties access to the equipment as part of an unauthorized "audit" following the 2020 election. And in Ohio, the election system of one county was part of an attempted breach that investigators believe was assisted by a worker inside the office. While the investigation has not yet shown that sensitive information was compromised, data from the laptop were later shared at an election conspiracy conference hosted by prominent election conspiracist Mike Lindell.

Federal and state government entities must act now to respond to these insider threats. The first state to do so this year was Colorado. Following the notoriety of the Tina Peters case, Colorado passed a new law increasing internal election security measures. Provisions in the new law include making it a felony to facilitate unauthorized access to voting equipment, as well as requiring all county election clerks to install round-the-clock video surveillance of voting system components and key-card access points to rooms where that equipment is kept. The federal Cybersecurity and Infrastructure Security Agency (CISA) has also responded to these insider threats, releasing new guidance that urges all states to adopt policies similar to those contained in the new Colorado law. The Bipartisan Policy Center also released a report with recommendations focused on the partisanship of election officials; suggested policies include discontinuing the use of partisan elections to select election officials and codifying ethical requirements that such officials do not engage in political activity and have a certain level of experience and qualification.

Along with protecting election officials who act in good faith from threats and harassment, states must also act to prevent bad faith actors from sabotaging the security of our elections from the inside. The number of election denialists running for positions that control election administration across the country poses a true threat in 2024 if these partisan actors take office. Implementation of proactive policies, such as the law enacted in Colorado, can prevent disaster for our democracy in the future.

Election Security Approach #3: Modernizing Voter Registration

Voter registration policies such as automatic and online registration work to determine the eligible electorate in each state, which is often unduly restricted before elections even begin. Modernizing state voter registration systems improves election security while also increasing accessibility and lowering barriers to voting. While paper-based systems can be good practice for ballots themselves, the voter registration process can be improved by moving to electronic systems that increase accuracy of voter rolls, lower costs, and improve access. In particular, there are three main policies states can adopt to modernize their voter registration systems: automatic voter registration, membership in the Electronic Registration Information Center, and online voter registration.

Automatic Voter Registration

Automatic voter registration (AVR) helps to modernize voter registration by automatically registering eligible voters through their interactions with state agencies. While adopting any form of AVR represents a step forward, there are different approaches to implementing the policy that make a significant difference: "front-end" vs. "back-end" AVR. In front-end systems, the voter is given an opportunity at the time of their interaction with a state agency to decide whether to opt-out of being registered. In back-end systems, state agencies send information from these transactions to state election authorities. The voter is then automatically registered and then given an opportunity to opt-out later. Whether states utilize "front-end" or "back-end" AVR matters. Recent studies show that implementing back-end AVR results in an 8.1% increase in registration, compared to 2.9% for front-end AVR. The use of back-end of AVR significantly improves the security of a state's election system. Front-end systems present more opportunities for errors, particularly in relation to the inadvertent registration of non-citizens who may, for example, agree to be registered without fully understanding they are registering to vote, despite coming in to renew their driver's license. Such mistakes can further diminish public trust in our election systems. In contrast, back-end AVR improves election security by preventing non-citizens from inadvertently registering to vote. People who are not citizens are automatically filtered out of the voter registration process. AVR, specifically back-end, is a policy that modernizes voter registration while improving security and access simultaneously. For more information on AVR best practices, see our recent policy spotlight.

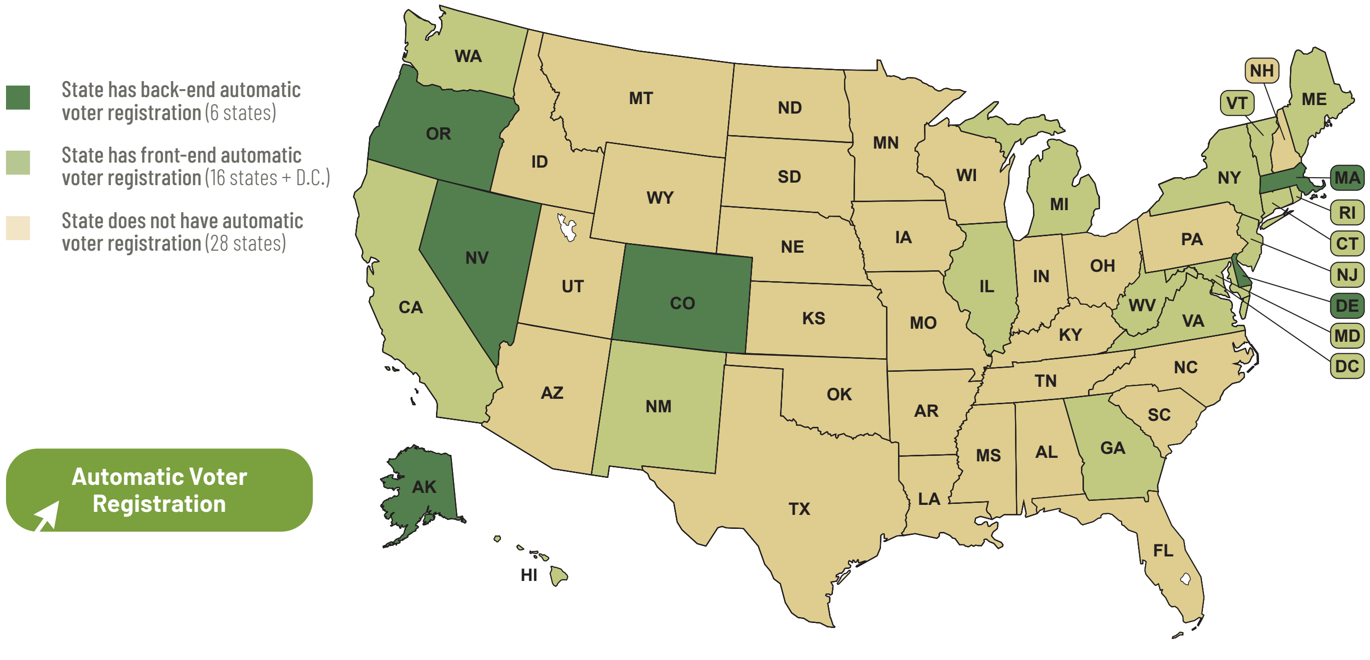
> *Whether states utilize "front-end" or "back-end" AVR matters. Recent studies show that implementing back-end AVR results in an 8.1% increase in registration, compared to 2.9% for front-end AVR.*

As shown in **Figure 2**, 22 states and D.C. have some form of automatic voter registration, but only six of those states have implemented a back-end process. Despite this progress, more than 50% of eligible voters live in states that have not adopted AVR.

Accurate Voter Lists

One of the first steps in running a secure election is having accurate and updated voter rolls. The Electronic Registration Information Center (ERIC) is a non-profit organization created to assist states in improving the accuracy of their voter rolls. ERIC helps states modernize their voter registration systems and increase efficiency and security.

FIGURE 2: AUTOMATIC VOTER REGISTRATION


State has back-end automatic voter registration (6 states)
State has front-end automatic voter registration (16 states + D.C.)
State does not have automatic voter registration (28 states)
Automatic Voter Registration
WA
OR
CA
NV
ID
MT
WY
UT
CO
AZ
NM
AK
HI
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MI
IN
OH
KY
TN
MS
AL
GA
FL
SC
NC
VA
WV
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC

Member states submit their data to ERIC which then allows the states to see if voters have moved within or out of state, identify duplicate registrations and remove ineligible voters. Like automatic voter registration, ERIC leverages electronic technology instead of outdated paper-based systems. It also allows state agencies to share information with other member states, resulting in more accurate voter lists while also conserving resources. As shown in **Figure 3**, 32 states and the District of Columbia are currently members of ERIC, representing 65% of eligible voters.

Online Voter Registration

Online voter registration (OVR) was one of the first policies designed to modernize the voter registration process. OVR, like AVR and membership in ERIC, evolves registration beyond paper-based systems and allows voters to fill out and submit registration forms electronically through secure online portals set up by their state. In most states, these systems work in tandem with, and are checked against, information from driver's licenses or other state-issued IDs. Online voter registration increases the convenience, accuracy, and efficiency of our election systems by avoiding errors that are common on paper forms and reducing the burden on election officials to process those forms.

As shown in **Figure 4**, 42 states allow online voter registration, which represents almost 90% of eligible voters.

The three policies discussed in this section represent some of the best options for states to modernize their voter registration systems and thereby greatly improve the security of their election systems while also maintaining and even increasing access for voters. By adopting these policies, states can increase the number of registered voters, preserve election officials' time and resources, and increase security.

FIGURE 3: MEMBERSHIP IN ELECTRONIC REGISTRATION INFORMATION CENTER (ERIC)

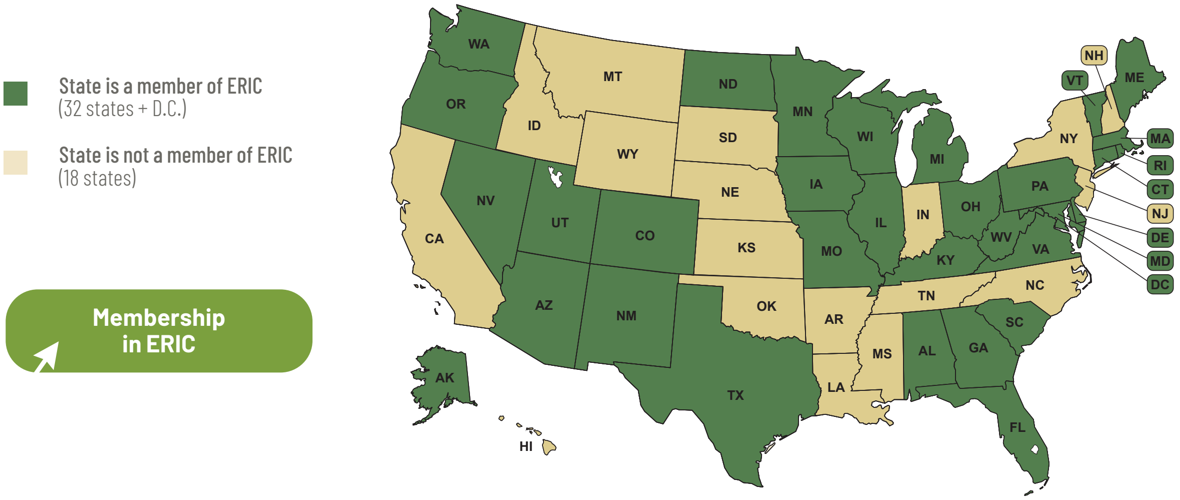
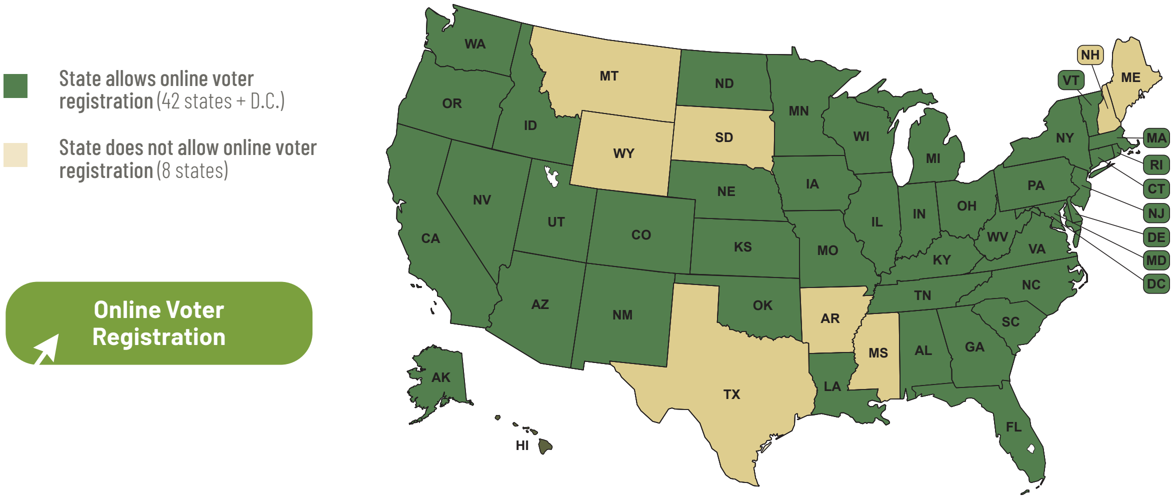


FIGURE 4: ONLINE VOTER REGISTRATION


🟩 State allows online voter registration (42 states + D.C.)
State does not allow online voter registration (8 states)
Online Voter Registration
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC
AK
HI

Election Security Approach #4: Secure Technology for In-Person and Mail Voting

In addition to implementing policies to secure the processes leading up to and following an election, it is important for states to also address security in the context of in-person and mail voting. In terms of in-person voting, the most important area in which states can dictate policy relates to the security of voting machines and the use of voter-verified paper ballots. Mail voting, which in itself improves security by necessitating the use of paper ballots, can also be further secured through the use of technologies like ballot tracking.

Secure Voting Machines and Voter-Verifiable Paper Ballots

States vary widely in the types of voting machines used for in-person voting. The most secure systems use paper ballots where the voter hand-marks their choices. States with secure voting machines are defined by security experts such as Verified Voting as systems that use hand-marked paper ballots for most voters. Paper ballots are more resistant to tampering and potential external and internal security threats –and the paper trail they provide makes it easier to conduct routine audits to verify results.

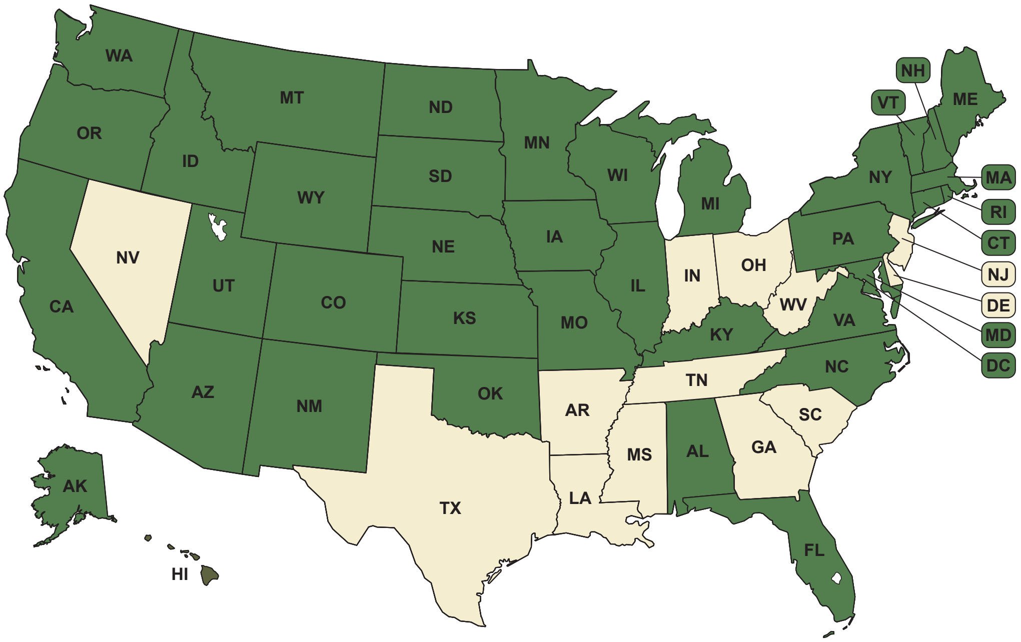
In 37 states and D.C., the majority of voters can use secure voting technology with a verifiable paper trail. But in 13 states the majority of voters are not able to use secure voting technology with a verifiable paper trail, as shown in **Figure 5**.

In states that do not use paper ballots for most voters, ballots are often cast on ballot marking devices (BMDs) or direct recording electronic systems (DREs). BMDs are a type of voting machine through which a voter is presented with an electronic screen showing their ballot options, and then some form of a printed record is produced. Security experts have pointed out flaws with some BMDs in that they do not always produce a record that is verifiable by the voter—sometimes the resulting printout simply contains a barcode or other information that is not readable. BMDs were created as a result of requirements in federal law that all polling places have accessible options for disabled voters to be able to mark their ballot privately and independently, so it is

FIGURE 5: SECURITY OF VOTING MACHINES (HAND MARKED PAPER BALLOTS)

🟩 Majority of voters in the state can use secure voting machines (37 states + D.C.)

⬜ Majority of voters in the state cannot use secure voting machines (13 states)



Security of Voting Machines

important to maintain this option. However, security experts recommend that when BMDs are used, they should produce a verifiable paper ballot rather than a summary or other information.

The final type of voting equipment used in the states, although they are used relatively infrequently today, are DREs. These voting machines operate on an entirely electronic interface where the voter's selections are stored on computer memory. These systems do not use paper ballots and are therefore considered one of the least secure options by election security experts.

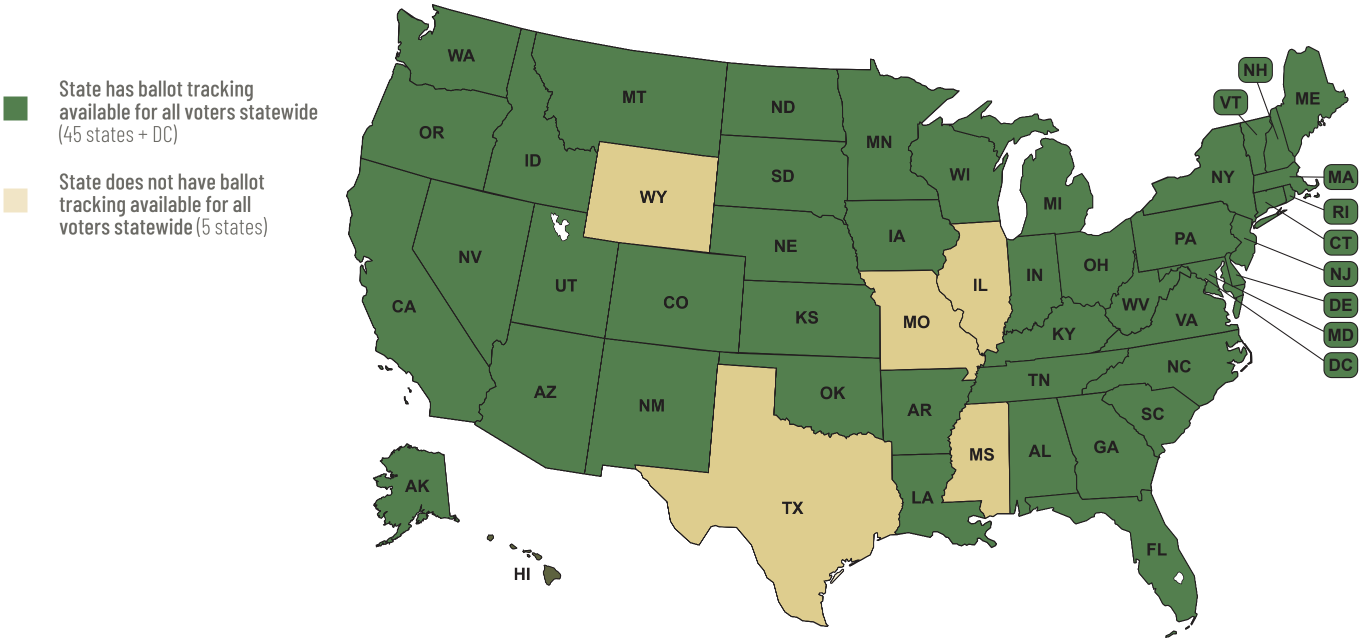
Security of Mail Voting

The past decade has also seen the growing adoption of policy options for voters to cast their ballots outside of the polling place, through mail voting. While there have been numerous false allegations since the 2020 election that mail voting increases the potential for fraud, the opposite is true. Mail voting has been used since the Civil War; the first absentee voters were soldiers casting their ballots from the battlefield. Multiple features of mail voting contribute to increased election security, most notably that such a voting system requires the use of voter-verifiable paper ballots. Mail ballots are also returned in sealed envelopes and usually contain a voter's signature, which provides an additional layer of security. One increasingly popular policy that could further improve security related to mail voting is online ballot tracking. These systems often allow a voter to track their ballot through each step of the election process, from mailing until it is verified and counted. Ballot tracking systems also allow election offices to keep track of ballots and prevent opportunities for ballots to be lost or misused.

> *Mail voting has been used since the Civil War; the first absentee voters were soldiers casting their ballots from the battlefield.*

As shown in **Figure 6**, nearly every state allows all voters to track the status of their vote by mail ballot to ensure confidence that it was received and counted. Only five states — Illinois, Mississippi, Missouri, Texas, and Wyoming — don't allow all voters to track the status of their mail-in ballot.

FIGURE 6: BALLOT TRACKING FOR MAIL VOTING


🟩 State has ballot tracking available for all voters statewide (45 states + DC)
🟨 State does not have ballot tracking available for all voters statewide (5 states)
WA
OR
CA
AK
HI
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
PA
VA
NC
SC
NY
NH
VT
ME
MA
RI
CT
NJ
DE
MD
DC

Ballot Tracking for Mail Voting

Election Security Approach #5: Appropriate Use of Post-Election Audits

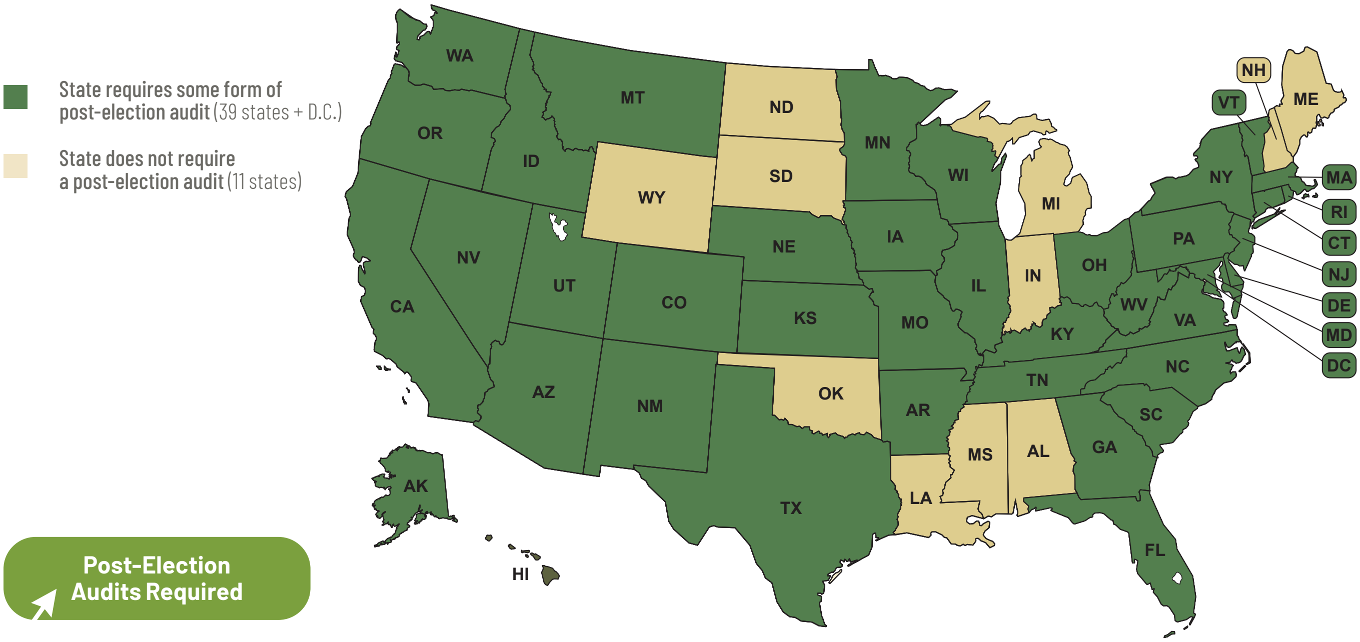
Post-election audits, when properly utilized, are a nonpartisan tool that allows states to verify the accuracy and performance of voting equipment and vote counting machines. In effect, a post-election audit is a partial recount of results, checking random samples of paper ballots or records against the results produced by the voting system, to verify that the voting system accurately recorded and counted the votes. There are also best practices, specifically the use of risk-limiting audits, that states can adopt to ensure the utmost level of confidence in election results. Properly conducted, nonpartisan audits provide public confidence in election results and can also act as a safeguard against hacking and foreign interference by identifying potential anomalies in vote counts.

This kind of legitimate nonpartisan audit is a best practice that is currently utilized in 39 states and the District of Columbia, as shown in **Figure 7**. This means that 88% of eligible voters live in a state that is already taking this important measure to ensure the integrity and accuracy of election results.

Since the 2020 election, partisan officials have hired unqualified individuals to conduct improper ballot reviews in states like Arizona and Wisconsin, not because of any evidence that a larger review is needed, but simply because they were unhappy with the election results and wanted to undermine trust in state voting systems and election officials. These efforts, which in some cases have compromised the integrity of both ballots and voting machines, should not be characterized as audits, as they were designed and undertaken for illegitimate purposes.

The primary distinguishing factors between legitimate and illegitimate use of audits are that legitimate audits are conducted under routine schedules by government entities, with election workers operating in bipartisan teams, and following strict security procedures that maintain ballot chain of custody. Legitimate audits can also occur in cases of very close election results, or if a routine or risk-limiting audit shows an anomaly that suggests the need for a more detailed review. Illegitimate audits, such as the one conducted in Arizona by the unqualified outside group Cyber Ninjas, are often initiated for partisan reasons, outside of routine schedules and using unsecure procedures that open up voting machines to cyber vulnerabilities and violate chain of custody while potentially exposing personal information of voters.

FIGURE 7: POST-ELECTION AUDITS REQUIRED


🟩 State requires some form of post-election audit (39 states + D.C.)
🟨 State does not require a post-election audit (11 states)
WA
OR
CA
AK
HI
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
GA
FL
WV
VA
NC
SC
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC

Post-Election Audits Required

Risk-Limiting Audits

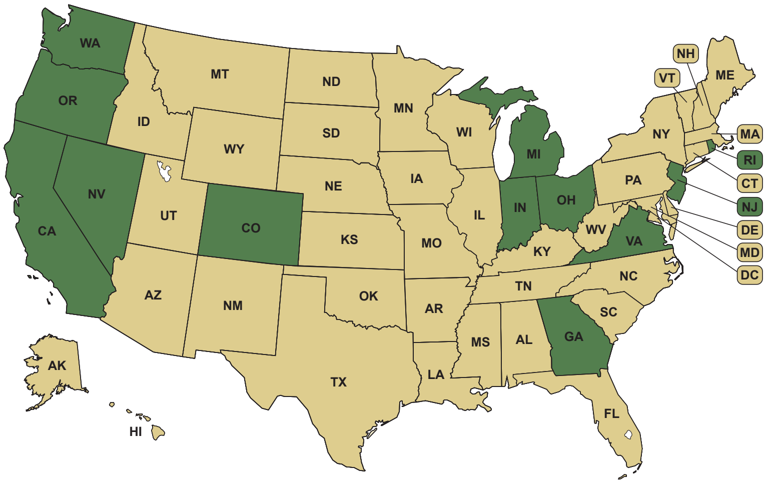
While most states require some form of a routine post-election audit, the current consensus among election and security experts, including the American Statistical Association, is that the best practice is to implement risk-limiting post-election audits. Risk-limiting audits are a form of audit that uses statistical methods to analyze random samples of ballots and verify the accuracy of election results. In a risk-limiting audit, the size of the random ballot sample is increased until there is statistical and objective confidence in the election results. Risk-limiting audits can also preserve resources and time as they operate by examining more ballots in the context of a close election, while less examination is needed to confirm statistical confidence in contests with wide margins. Legitimate post-election audits, specifically risk-limiting audits, are a commonsense policy solution that bolsters public confidence in election results and improves the security of election systems.

Currently, only 12 states utilize risk-limiting audits as a regular part of their elections process, as shown in **Figure 8.**

FIGURE 8: RISK-LIMITING AUDITS

🟩 State conducts risk limiting audits (12 states)

🟨 State does not conduct risk limiting audits (38 states + DC)



Risk-Limiting Audits

The Fraudulent Narrative of Voter Fraud

Election security has become a controversial topic in today's polarized landscape, with some Republican officials advocating for restrictive voting policies under the guise of reducing "voter fraud." The policies discussed in this report, such as legitimate post-election audits and AVR, are proven to increase election security while preserving accessible voting options. In contrast, many policies currently being pushed by Republican lawmakers, such as strict voter ID laws and bans on ballot drop boxes, have no impact on election security but rather disenfranchise voters. According to an Associated Press review of voter fraud allegations in the 2020 election that examined more than 25 million votes in battleground states, only 425 potential cases were identified—far too few to make a difference in any state in 2020. In addition, data from the conservative Heritage Foundation's voter fraud database (which includes non-voting offenses such as submitting false signatures for ballot petitions) show no meaningful difference in the amount of fraud between states. In other words, states with expansive voter ID options and no-excuse mail voting laws had the same level of voting integrity as states with strict voter ID requirements and restrictions of mail voting. According to an analysis of the Heritage database in 2017 by the Brennan Center, there were only 51 cases of alleged voter fraud in decades of records that would have been prevented by restrictive policies such as requiring photo identification. In reality, restrictive policies suppress turnout and result in millions of citizens facing undue challenges in exercising their right to vote.

Conclusion

Our democracy has arguably never been under greater threat than it is today, less than two years removed from an election in which the former president made false claims of massive voter fraud. These claims led to an increase in political violence and culminated in the attack on the Capitol on January 6, 2021. Despite these looming threats, a significant portion of Republican lawmakers across the states have leaned into election denial and continue to advocate for policies that do not actually address election security but instead work to restrict access for voters, policies that are particularly notable in the wake of the highest turnout election in modern history. Fortunately, there are policies that states can adopt that actually improve election security while maintaining and even increasing access for voters. By adopting common sense reforms like automatic voter registration, risk-limiting audits, and working to prevent external and internal threats to elections, our democracy can be preserved.