TESTIMONY OF
GOWRI RAMACHANDRAN

SENIOR COUNSEL, DEMOCRACY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW

HEARING ON
SECURING DEMOCRACY: PROTECTING AGAINST THREATS TO ELECTION INFRASTRUCTURE AND VOTER CONFIDENCE

THE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, & INNOVATION
U.S. HOUSE OF REPRESENTATIVES

JANUARY 20, 2022
Chairwoman Clarke, Ranking Member Garbarino, and members of the Committee:

Thank you for the opportunity to discuss the security of our nation’s election infrastructure. Despite a global pandemic, the November 2020 election saw historic turnout and was widely considered the most secure in American history.\(^1\) But an anti-democracy movement, fueled by the Big Lie, poses serious threats to the security of elections. Taking these threats seriously means building upon recent improvements to election infrastructure security, such as the increased use of auditable paper ballots and increased information sharing between state and local election officials and the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

The Brennan Center for Justice—a nonpartisan law and policy institute that focuses on democracy and justice—appreciates the opportunity to report on the security of our election infrastructure, threats to that infrastructure, and ways to secure against these dangers. At the Brennan Center, I focus on election security, and I frequently engage with state and local election officials to advocate for and assist with the implementation of election security and resiliency measures.\(^2\)

In my testimony, I will cover three topics. First, I will describe what went right in 2020. This included the widespread use of auditable paper ballots, cooperation between state and local election officials and CISA, resiliency measures and money from Congress to ensure voters could exercise their rights safely in a pandemic, and the resiliency of voters themselves, who made thoughtful plans to vote safely and securely. This was all followed by routine, statutory tabulation audits in every swing state, finding no discrepancies sufficient to change the outcome of the Presidential election.

Second, I will describe the threats that the election sabotage movement is posing to election infrastructure. These threats include sham partisan reviews that undermine confidence

---

and security,3 violent threats and intimidation of election officials and workers,4 and the potential infiltration of election offices, polling places, and election vendors by anti-democratic forces.5 Of particular concern: Candidates for election administration positions are raising unprecedented sums as they campaign on election denial.6

Third, I will address how election infrastructure can be bolstered against this threat. Online platforms and traditional media should work with civil society to ensure they are promoting accurate election information.7 Existing laws against intimidation, coercion, and threats should be enforced,8 and states should, with support from Congress, consistently adopt traditional guardrails against insider threats. These include restricting and logging access to critical systems, using transparent procedures such as nonpartisan and bipartisan election observation, monitoring for inappropriate activity, requiring vendors to follow cybersecurity, personnel, and supply chain standards, and removing any officials or workers who actively undermine election integrity.9 Congress should mandate and provide incentives for true election integrity measures, such as risk-limiting audits, rigorous election vendor standards, and independent security testing, as the Freedom to Vote: John R. Lewis Act does.10

I. WHAT WENT RIGHT IN 2020

The November 2020 election was the most secure election in American history, with the highest turnout since 1900.11 This was accomplished through the heroic efforts of state and local

---

9 Elections Project Staff, “Election Observers are Official Actors that Promote Legitimacy and Transparency. They are Typically Appointed, Trained, and are Barred from Voter Intimidation by State and Federal Laws,” Bipartisan Policy Center, October 23, 2020, https://bipartisanpolicy.org/blog/election-observers-are-generally-appointed-and-are-held-to-strict-standards-of-behavior.
11 Women, Asian Americans, and Native Americans were not able to vote in 1900. U.S. Const. amend. XIX (ratified Aug. 18, 1920); Terry Ao Minnis and Mee Moua, “50 Years of the Voting Rights Act: An Asian American
election officials, their staff, and pollworkers, with support from CISA, the Election Administration Commission (EAC), Congress, civil society, and voters themselves.

A. An Estimated 96 Percent of Voters Used Voter-Verifiable Paper Ballots

In order to demonstrate the trustworthiness of elections, election officials need auditable, voter-verifiable paper ballot systems.\(^{12}\) These allow for routine, statutory post-election tabulation audits, in which a sample of paper ballots are compared to the machine-tabulated results. These types of audits are designed to catch tabulation errors, whether they might be the result of malicious activity or technical errors. When these types of audits are routinely performed by competent administrators in a transparent manner, they can and should boost confidence in the accuracy of electoral outcomes. The Brennan Center and others have long advocated for this type of audit.\(^ {13}\)

In 2016, one in five voters cast their vote using a paperless voting system that could not be subject to a tabulation audit.\(^ {14}\) But thanks to election officials across the country transitioning to more secure systems that scan paper ballots, as well as the choice of more voters to vote by mail during the pandemic, an estimated 96 percent of voters used voter-verifiable paper ballots in the 2020 election. No swing state used paperless voting machines.\(^ {15}\)

B. CISA and State and Local Election Officials Cooperated To Prevent, Detect, and Recover from Cyberattacks


CISA established a partnership with and supported state and local election officials in the years and months leading up to the 2020 election by providing vulnerability testing, promoting best practices for resiliency, and providing trainings, such as tabletop exercises in which officials practiced responding to security breaches.

CISA also ramped up its information sharing with state and local election officials, and the public, and this information sharing paid off. For instance, in the fall of 2020, some Florida voters received threatening and intimidating emails in the guise of a far-right group that has promoted violence. The intelligence community detected the true source of the attack, and CISA, the FBI, and the Office of the DNI held a joint press conference to let the public know the truth: that the emails were coming from malicious actors associated with Iran. By quickly informing the public, they were able to reduce any intimidating effect. As Director Ratcliffe stated on October 21, 2020, “These actions are desperate attempts by desperate adversaries. . . . We ask every American to do their part to defend against those who wish us harm. The way you do that is quite simple: Do not allow these efforts to have their intended effect. If you receive an intimidating or manipulative email in your inbox, don’t be alarmed, and don’t spread it.”

A few days later, CISA and the FBI issued a public alert, notifying Americans that malicious actors, including some associated with the Iranian government, were scanning multiple states’ election webpages for vulnerabilities, and that one state’s voter registration data had successfully been accessed. Shortly thereafter, Florida closed down its statewide page with a voter information lookup tool and informed voter advocates who objected that the closure was...
due to a security vulnerability. Advocates were able to secure modifications to the page that did not re-open the security vulnerability, but ensured voters with questions could still obtain the information they needed, such as their polling place location.23

C. Resiliency Measures and Money from Congress Helped Americans Vote Safely Despite Pandemic

CISA, election security experts, and voting rights advocates all encouraged the adoption of resiliency measures to help election officials detect, prevent, and importantly, recover from an attack or technical failure.24 Many election officials employed these measures, including the maintenance of emergency paper ballots, to be used in case ballot marking devices malfunctioned,25 as well as keeping paper pollbook backups in polling places that use electronic pollbooks,26 in case of a malicious attack or malfunction of the electronic books. Provisional ballots were also kept on hand in case an attack or malfunction prevented pollworkers from confirming a voter’s eligibility to vote in real time.27 Each of these resiliency measures came in handy in at least some locations, helping ensure that voting could continue and voters did not need to be turned away, even when occasional hiccups with equipment occurred.28

In addition to these resiliency measures against electronic equipment failures, the provision by many states of multiple options for voting – in person Election Day, in person early, and mail voting – served as its own resiliency measure against the pandemic. These options

---


allowed voters to spread themselves out among different voting methods and days, thereby reducing crowds at polling places for the increased safety of all. They also allowed voters to, if faced with a long line due to some technical issue during early voting, return on another day when the problem had been ameliorated.\textsuperscript{29} They also meant election officials needed resources – from personal protective equipment for pollworkers and voters voting in person, to extra supplies given uncertainty about which voting methods voters would use and larger facilities for workers to socially distance in while processing and tabulating mail ballots.\textsuperscript{30} The resiliency measures that election officials employed and the money that Congress provided to help pay for them was crucial in running a safe and secure election.\textsuperscript{31}

D. Legitimate Post Election Audits and Recounts Confirmed that Outcomes Were Correct

Finally, after Election Day came and went, routine, statutory tabulation audits were performed in every swing state, with additional recounts in some. None found discrepancies that would have been sufficient to alter the outcome of the Presidential election, thereby providing added confidence in the integrity of the election.\textsuperscript{32}

Of course, there is room for improvement. Ideally, all states would conduct routine, statutory tabulation audits with the opportunity for nonpartisan and bipartisan observation. In these audits, a sample of ballots would be compared to machine counts, and ideally, they would include risk-limiting audits. In a risk-limiting audit, the number of ballots sampled varies based on how close the contest being audited is, in order to provide a pre-determined statistical level of confidence that any discrepancies were not sufficient to alter the outcome.\textsuperscript{33}

Currently, most states have some kind of routine post-election tabulation audit, and only a few states conduct risk-limiting audits.\textsuperscript{34} Requiring risk-limiting audits is an example of the kind of measure that could truly improve upon election integrity, as opposed to sham partisan

\textsuperscript{29} Córdova McCadney, Tisler, and Norden, “2020’s Lessons for Election Security.”
\textsuperscript{31} Córdova McCadney, Tisler, and Norden, “2020’s Lessons for Election Security.”
\textsuperscript{32} Bydlak et al., Partisan Election Review Efforts in Five States.
reviews,\textsuperscript{35} laws that make it easier for monitors to interfere with and disturb election administration,\textsuperscript{36} or laws that make it impossible for election officials to assist and educate voters about their rights.\textsuperscript{37}

II. THREAT OF ELECTION SABOTAGE

It is imperative that all those who worked to secure our election infrastructure against the threat of foreign interference and attacks in 2020 continue those efforts. But the events of the past year have shown that there is a fast-growing threat of election sabotage from an anti-democratic movement within our own country, and that this threat also deserves focus. In fact, the two threats could compound each other, with homegrown election conspiracies making it easier for foreign governments and their agents to accelerate destabilization merely by seeding and amplifying doubts and confusion, rather than investing in developing sophisticated cyberattacks.

The domestic anti-democracy movement also threatens election infrastructure directly, through sham partisan reviews that undermine not only confidence but security, and through a variety of threats to the integrity of the people who make up our election infrastructure – election officials, election workers, and election vendor personnel.

A. Sham Partisan Reviews Undermine Security

Loyalists of former president Donald Trump invaded the U.S. Capitol one year ago, carrying weapons, waving the Confederate flag, and insisting that the 2020 election was fraudulent. There was no credible support for the claims of “Stop the Steal” advocates. Nevertheless, Pro-Trump politicians have spent the past year attempting to fabricate that support. They have dented public confidence in the voting process and made it harder for voters, in particular voters of color, to vote. Less recognized, but no less damaging, is the way they have coopted and undermined a critical tool of our democracy: the post-election audit.\textsuperscript{38}

Many states have rigorous protocols for post-election audits, including randomized selection of the electronic tallies to be checked against paper records, a commitment to objectivity throughout the process, and conducting the audit in full public view.\textsuperscript{39} When these standards are upheld, post-election audits help check that the outcomes of elections are accurate, and they maintain or restore public confidence in our democracy. The sham reviews following


\textsuperscript{39} National Conference of State Legislatures, “Post-Election Audits”; and Howard, Rivest, and Stark, \textit{A Review of Robust Post-Election Audits}. 
the 2020 election are, essentially, the opposite of this. They were initiated for partisan reasons, as part of an attempt to overturn the will of the voters.

They can also undermine security by providing unmonitored access to systems to biased partisans, leading to equipment no longer being safe to deploy in future elections. Ballot security breaches are another damaging effect, with inexperienced partisans permitting those handling the ballots to use pens that could change the vote records. They have also threatened potential voter intimidation with plans for biased partisans to knock on voters’ doors asking questions. These security problems with partisan reviews are exemplified in the movement’s most prominent effort to date: the partisan review of Maricopa County’s 2020 election, conducted by the contractor Cyber Ninjas. Cyber Ninjas finally issued a report in September 2021, replacing the outright lies that have triggered defamation lawsuits against other Big Lie proponents with copious and misleading innuendo. The Maricopa County Recorder, Stephen Richer (R), recently issued a lengthy point-by-point rebuttal, in which the county identified 75 claims made by the audit team and debunked them all. The county’s analysis determined 38 were inaccurate, 25 were misleading, and 11 were false.

The contractors’ most attention-grabbing findings fit the pattern that purveyors of voter fraud myths have long followed: willful ignorance of basic probability, common election laws, and routine election administration procedures in order to raise baseless suspicions about
fellow voters and the dedicated public servants who count their votes and certify the results. The report claims it is suspicious that some voters share the same full name and birth year — it isn’t. It uses a commercial move tracking service to raise suspicions about voters who, according to the commercial service, moved before the election. But even leaving aside the accuracy of the commercial service’s data, temporary moves do not alter eligibility to vote in Arizona. Unsurprisingly, the Cyber Ninjas audit was promptly used in the continuing disinformation campaign against our elections, with Trump citing its “critical” — and false — “finding” that 23,344 ballots were somehow impacted by the voters purportedly moving.

The push to conduct partisan reviews continues to spread. State legislators in Pennsylvania have proposed conducting their own partisan review that would use the Arizona Senate’s actions as a model. Assembly members in Wisconsin have launched a partisan effort there, targeting officials in its largest cities: Milwaukee, Madison, Racine, Kenosha, and Green Bay. Despite the dismissal of a lawsuit seeking to gain access to ballots in Fulton County, GA, for a partisan review, gubernatorial candidate David Perdue has sued Fulton County officials seeking a review. Now, even in states that President Trump won, such as Texas, Florida and Idaho, local party activists have demanded these reviews over the objections of local election supervisors of both major parties.

---

50 Ramachandran, “The Arizona’s Senate’s Contractors Fail to Understand Basic Probability and Voter Data.”
51 Howard and Ramachandran, “Partisan Arizona Election ‘Audit’ Was Flawed from the Start.”
B. Violent Threats and Intimidation, Along with Partisan Attacks, Are Pushing Out Personnel Committed to Free and Fair Elections

The Brennan Center for Justice commissioned a national survey of election officials this spring, which found that roughly one in three election officials feel unsafe because of their job, and approximately one in six listed threats to their lives as a job-related concern. This is unacceptable in a functioning democracy. The people who risked their lives during a pandemic to ensure that all eligible voters could vote, that they could vote safely, and that their votes would be counted accurately, cannot be subject to attacks and intimidation. Not only do they deserve better, but our democracy cannot survive when dedicated, honest people who provided the most secure election in American history, with the highest turnout since 1900 are subjected to death threats, simply for doing their jobs well.

The Department of Justice has created a task force to address the situation, but the overall lack of accountability for these bad actors continues to be dispiriting for the public servants who make our democracy function, and the impetus to step down is strong. In one recent example, despite having the support of at least one Republican Board of Elections member, Jeannetta


Thirty-two percent of election officials surveyed said that they felt unsafe because of their job. Seventeen percent of local election officials surveyed said that they had been threatened because of their job. Benenson Strategy Group, “The Brennan Center for Justice: Local Election Officials Survey,” April 7, 2021, https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey.


Watson, the first Black elections director in Macon-Bibb County, Georgia, stepped down last week. Board of Elections member Mike Kaplan said it was “a sad day for our country and especially Macon-Bibb,” as he “traced Watson’s troubles back to allegations of improper vote counting during the presidential election. Kaplan said workers were ‘followed home every night’ and under round-the-clock surveillance. ‘The stress and fear is too much,’ Kaplan said, adding that he believes Watson went through ‘a very contentious election where she was in fear of her life.’”

As one might expect, partisan attacks compound the many other pressures that election officials committed to nonpartisan election administration face, and many are being pushed out or resigning in the face of this pressure. Others are being stripped of their powers by partisan actors, in retaliation for certifying election results, or simply for being the face of nonpartisan election administration.

These attacks on election officials are a threat to the security of our election infrastructure, as officials who are committed to conducting free elections and respecting the will of the voters are themselves a crucial element of that infrastructure.

C. Elections Personnel Who Buy Into Conspiracies May Pose an Insider Threat

Unfortunately, almost one-third of Americans still believe the false narrative that the 2020 election was stolen, “a number that has not budged across five polls in which Monmouth [University Polling Institute] asked this question during the past year.” Given this fact, we shouldn’t be shocked that among the more than 8,000 local election officials — and tens of thousands of additional public and private sector employees that support their work — there are some who will also buy into these conspiracy theories. In fact, there has been an active effort to

---


63 Fabian, “Macon-Bibb Elections Supervisor Resigns, Cites Stress, Workload, New Election Laws.”

64 Wines, “After a Nightmare Year, Election Officials Are Quitting.”


recruit and convince election officials to facilitate these conspiracy theories and push the goals of election deniers. There is reason to worry these efforts could gain traction and followers in the election official community, posing yet another threat to the integrity of the human component of our election infrastructure. Those who work for election vendors may also be at risk.

Officials who have promoted election denialism may be especially susceptible to entreaties that they give unauthorized access. We are witnessing the first glimpses now. In Colorado, a county clerk with connections to election conspiracy theorists gave unauthorized access to the county’s Dominion voting systems—a vendor targeted by many proponents of the Big Lie. This access allowed the unauthorized person to take photos of passwords for the voting machine software, which then ended up online. The secretary of state decertified the county’s voting equipment and ordered the county to replace the machines before the next election.

In Michigan, a town clerk who shared election conspiracies on social media and who took office in 2021 refused to allow a vendor to perform routine maintenance on a voting machine because the clerk falsely believed the maintenance would erase old data that could prove the machines were rigged. When a central component of that machine went missing, the state police opened a criminal investigation into the clerk to locate the since-found equipment and determine whether the equipment had been tampered with.

---


69 Norden, Ramachandran, and Deluzio, A Framework for Election Vendor Oversight.


In Ohio, an individual inside a county commissioner’s office connected a private laptop to the county network in an attempted breach that state officials believe a government employee may have facilitated.\textsuperscript{74} While the connection did not allow access to voting systems, and no sensitive data appears to have been obtained, network traffic captured by the laptop was nonetheless shared at a conference hosted by election conspiracist Mike Lindell — the same conference where information from the Colorado breach was released. Officials in both counties had previously discussed baseless claims about the 2020 election with associates of Lindell.\textsuperscript{75}

D. Candidates Are Running for Election Administration Positions with Big Lie Messaging

The magnitude of the insider threat that anti-democracy forces could pose is clarified by examining races for governor, secretary of state, and local election administrator positions. There are thousands of local election jurisdictions in the United States, and in the vast majority of them, an elected individual is in charge.\textsuperscript{76} In past years, the question of who ran and certified our elections has traditionally been of little interest to most. But now, there is an alarming trend of candidates running on (and against) “election denialism.”\textsuperscript{77}

A preliminary Brennan Center analysis of campaign finance disclosures and messaging by candidates in swing states has found that much of the political discussion this year, 2022, is shaping up to be about 2020 and 2024: specifically, the Big Lie that the election was “stolen” from former President Trump in 2020, and that if he runs again and loses in 2024, those election results should be overturned.

So far, across three states with data available, fundraising in secretary of state races is two and a half times higher than it was by the same point in either of the last two election cycles. And campaigns are making election denial—and opposition to it—a key campaign issue in all

---


\textsuperscript{75} Gardner, Brown, and Barrett, “Attempted Breach of Ohio County Election Network Draws FBI and State Scrutiny.”


\textsuperscript{77} Vandewalker and Norden, “Financing of Races for Offices that Oversee Elections: January 2022.”
six of the battleground states with elections for secretary of state in 2022 — Arizona, Georgia, Michigan, Minnesota, Nevada, and Wisconsin.

In the contest for Georgia secretary of state, four candidates have each raised more than the 2018 winner had at this point, and the candidate raising the most money has refused to acknowledge that Joe Biden won the 2020 election. The Georgia election also features an early indication that these contests are being nationalized. The portion of funding in the race from out-of-state donors so far, 22 percent, is a marked increase over 2018, when it was 13 percent, and more than four times the amount from 2014, which was only 5 percent.

In Michigan, the incumbent has raised $1.2 million — six times what the last incumbent had raised at this point in 2014. This candidate is running against election denialism, against an opponent who has said voting machines in the state could have flipped 200,000 votes to Joe Biden.

Regardless of who enjoys a fundraising advantage in any particular state, voters are likely to be exposed to unprecedented amounts of political spending on the issue of election denialism, with it no longer being taken as a given that elections will be administered in a nonpartisan manner, regardless of the identity of the administrator.

III. WHAT CAN BE DONE

Lawmakers should support the excellent work that CISA, the EAC, and state and local election officials have done to further election integrity. But they should also act now to further mitigate these growing security risks posed by domestic anti-democracy forces. There are a variety of broadly accepted methods for mitigating insider threats, which state and local jurisdictions should adopt, and on which Congress can lead by providing the needed financial support. Congress can also provide support for the physical safety and security of elections personnel and elections offices, as well as for risk-limiting audits—a true election integrity

83 Vandewalker and Norden, “Financing of Races for Offices that Oversee Elections: January 2022.”
84 Vandewalker and Norden, “Financing of Races for Offices that Oversee Elections: January 2022.”
85 Vandewalker and Norden, “Financing of Races for Offices that Oversee Elections: January 2022.”
measure. Others can do their part as well: Online media platforms and traditional media can work with civil society to ensure they are promoting the most accurate information, and law enforcement at all levels of government can take threats against election administration seriously, enforcing the laws that exist to deter these crimes.

A. Congress Should Provide Support for Mitigating Insider Threats, Including Against Vendors

Insider threat risks have been a central focus of security efforts in other sectors, and best practices, such as those from the Cybersecurity and Infrastructure Security Agency, exist to prevent and respond to this activity.86

Among other things that can be done to both secure election systems from insider threats and build public confidence that those systems can be trusted, states and counties should take the following actions, and Congress should provide resources to support these mandates, many of which require financial resources to implement consistently.

1. Restrict access to election systems.

Election officials should ensure that an individual only have access to critical systems — both physical and digital — if access is necessary for that individual to perform their official responsibilities, and only to the extent that those responsibilities require it (this is known as the “principle of least privilege”87). In addition, election officials should require all individuals that access critical systems to first complete a background check. A recent regulation in Colorado88, for example, restricts voting system access to individuals who have passed a background check and are employees of the county clerk, voting system provider, or secretary of state’s office.

Where possible, official procedures should require two people and/or bipartisan teams to be present when accessing election systems, ballots, and election records. Election staff should also be on site with private vendors at all times.89

2. Establish transparent procedures and monitor for inappropriate activity.

Transparency protocols helped officials in Colorado identify the source of leaked voting system information.90 A state investigation found that the county clerk gave an

89 Norden and Tisler, “Addressing Insider Threats in Elections.”
unauthorized person a key card, and this card was logged when the individual entered the election facility. The clerk had also blatantly flouted another transparency measure by turning off video surveillance of the voting machines before the breach. But if the information obtained from the breach had not been discussed so publicly, it’s possible the state would have missed this activity.

Election officials must adopt and actively review transparency protocols to ensure that every person who accesses election systems is authorized to do so. Funding should be provided for election officials to install key card access to facilities that hold voting systems, so that a log of every entry can be created. All election offices should be equipped with and require 24-hour surveillance of voting systems and ballots, that can be reviewed and compared with access logs in the event of unauthorized activity. Where possible, that footage should be stored for at least two years. Both the access logs and surveillance data should be made available to the state, and state officials should ensure that local offices have sufficient procedures in place to detect unauthorized access.

3. **Remove and prosecute officials and workers who actively undermine election integrity.**

When officials do discover wrongdoing, these individuals must be held accountable. States have different processes for removing election officials. In some cases, the entity that appointed an election official may simply fire that individual. In others, state officials may hold power to remove election administrators or strip them of election responsibilities. When officials do discover wrongdoing, these individuals must be held accountable. States have different processes for removing election officials. In some cases, the entity that appointed an election official may simply fire that individual. In others, state officials may hold power to remove election administrators or strip them of election responsibilities.91 Officials may also seek permission from courts to do so.92 State and local officials, as well as their attorneys, should be familiar with the removal options available and be prepared to take the steps necessary to protect our election infrastructure from insider threats.

Where appropriate, law enforcement officials should also pursue prosecution against election workers who tamper with or allow unauthorized access to voting systems and election materials. State laws may require updating to address this conduct.

4. **Increase resiliency against insider threats to vendors.**

Private vendors are involved at every stage of an election, from registering voters to counting ballots to reporting results. States can act now to establish standards on cybersecurity, personnel security, and supply chain integrity for their election vendors.93 Congress should, as the Freedom to Vote: John R. Lewis Act does, directly incentivize vendors to adopt these standards by limiting expenditures of federal funds to those vendors that conform to best practices, which can be promulgated by CISA.94

---

91 Oosting, “Clerk Decries ‘Tyranny’ After Michigan Strips Her of Running Election.”


94 Freedom to Vote: John R. Lewis Act § 3908.
5. **Build in contractual safeguards.**

Local election offices can also build in safeguards through contracts when purchasing equipment and services.\(^{95}\) As a rule, vendors should be held to the same or higher level of standards for access and transparency as county or state employees. This can include background checks and the requirement to always have a state or county employee present when vendors access critical systems. This can also mean restricting or eliminating remote access by vendors.

Some of these solutions require statutory or regulatory changes at the state level, but Congress can take a leading role in providing additional resources for election offices that implementing these changes will necessitate. Congress can also lead on building resiliency of election vendors, at a minimum by limiting the expenditure of federal funds to those vendors that agree to comply with best practices in security, including resiliency to insider attacks.

**B. Congress Should Provide Support for the Security of Election Officials and Workers**

Congress should provide resources to states, via the Election Assistance Commission, that can be used for safety training, including prevention and de-escalation training for election workers. Funds could also be provided for education and training for officials on how to protect one’s personal information, as well as for states to expand their address protection services to cover election officials and workers. The Freedom To Vote: John R. Lewis Act additionally makes it a crime to reveal the personally identifying information of election officials and pollworkers with the intent to threaten or intimidate them.\(^{96}\) Resources could also be used to improve the physical security of election offices.\(^{97}\)

**C. Online Platforms and Traditional Media Should Work with Civil Society**

The Brennan Center, along with many others, encourages social media and other online speech platforms, along with traditional media, to amplify and promote trusted, accurate information about elections.\(^{98}\) Typically, election officials are and will be trustworthy sources of information about elections. But given the threats to the integrity of election officials posed by candidates who actively promote election disinformation, online platforms and traditional media must prepare for the possibility of a high-level election official promoting disinformation. Nonpartisan and bipartisan civil society groups can serve as an additional trusted resource, to help social and traditional media be sure they are promoting the most accurate information.

**D. Existing Laws Should Be Enforced**

---


96 Freedom to Vote: John R. Lewis Act § 3102.


The Department of Justice, and local and state law enforcement and prosecutors, should enforce existing laws against intimidation, coercion, and threats. There must be consequences for attempting to interfere with free and fair elections. The Department of Justice has launched a task force to combat threats against election workers.99 State and local prosecutors should take these threats seriously as well.

For a recent example of law enforcement bringing charges against someone making threats against an election official, in Genesee County, MI, the chair of the County GOP has recently pled guilty to harassing the Houghton County clerk during her bid for re-election. The clerk initially reported that he called her at 1am, threatening to kill her dogs. The call was traced, a warrant was obtained for his phone records, and eventually he was charged and sentenced to a year of probation, 240 hours of community service, and a $650 fine.100

For an example of charges against someone threatening others over their defense of the integrity of the 2020 election, a man in California was recently sentenced to three years in prison after sending threatening messages to approximately 50 victims, “targeting those individuals because of their statements expressing that then-President Trump had lost the 2020 presidential election.”101

E. Congress Should Promote Legitimate, Risk-Limiting Audits

Another important security measure that guards against a variety of threats, including insider threats, is routine, statutory tabulation audits that include the opportunity for nonpartisan and bipartisan observation. Such audits can provide added confidence that a cyberattack, insider manipulation, or innocent programming error did not corrupt ballot scanners in such a way that the outcome of an election was altered. In particular, risk-limiting audits can provide a consistently high level of statistical confidence in the machine-tabulated outcome of an election contest.

Although at least 24 states as of 2020 had laws requiring routine post-election tabulation audits, only a few states conduct risk-limiting audits.102 Congress should require – and provide

99 U.S. Department of Justice, “Justice Department Launches Task Force to Combat Threats Against Election Workers.”
funding for risk-limiting audits of federal elections. This would be a positive improvement in election integrity, and it has received bipartisan support in the past.

IV. CONCLUSION

The heroic efforts of many, and in particular state and local election officials committed to free and fair elections, gave us a safe and secure election in November 2020 with historic turnout. Some crucial improvements in security and resiliency had been in the works for a number of years, such as states that transitioned to voting systems that scan paper ballots, or that took advantage of vulnerability assessments provided by CISA. Other resiliency measures had to be implemented in response to the pandemic and benefited from funding provided by Congress. This included increased mail ballot printing to accommodate increased demand from voters, as well as the purchase of secure dropboxes to permit those voters to safely drop off ballots outside. Longstanding best practices, such as the provision of emergency paper ballots, paper pollbook backups, and pollworkers on standby, took long hours and plenty of financial resources to implement during an extremely high-turnout election with added pandemic-related costs. Carrying out these practices demonstrated a commitment by election officials to ensure eligible voters would not be turned away, even in the case of malfunctioning equipment or a potential cyberattack.

Now, the disinformation campaign that has sowed distrust in that election has seeded an anti-democracy movement that poses significant threats to our election infrastructure. The threats include sham partisan reviews that undermine ballot and election equipment security, while further fueling the disinformation campaign. They also include attacks on election officials and workers that push out and disempower the very people who administered a historically secure election in 2020. And there may be insider threats from those who seek to replace them. Some who are running for election official positions are themselves promoting election conspiracies in their campaigns, highlighting how election officials themselves, election workers, or election vendor personnel can fall victim to and push conspiracies about the 2020 election. These insiders could be susceptible to requests for unauthorized access and other security breaches, as we’ve seen occur in a few jurisdictions already.

Maintaining a secure election infrastructure will require effort from many parts of society in the weeks and months to come. Congress can lead the way in this effort, by providing resources for states and local jurisdictions to implement measures that protect against insider threats, such as video surveillance of election equipment and background checks for personnel. Congress should also, as the Freedom to Vote: John R. Lewis Act does, incentivize election vendors’ adoption of best practices for personnel and supply chain security, by requiring that federal funds spent on election vendors go to those who agree to abide by these security measures, and by requiring risk-limiting audits in federal elections. Unlike sham partisan reviews, these would be true election integrity improvements.

103 Freedom to Vote: John R. Lewis Act, § 4001.
Congress should further provide resources for the physical and personal security of election officials, workers, and their offices, while state, local, and federal law enforcement should treat those who threaten and interfere with fair election administration as the serious threat to democracy that they are. Existing laws must be enforced against these bad actors.

Our election infrastructure is strong, as shown by the 2020 election, but it is facing a growing anti-democracy threat from within. Congress should protect democracy from that threat by investing in true election integrity measures.