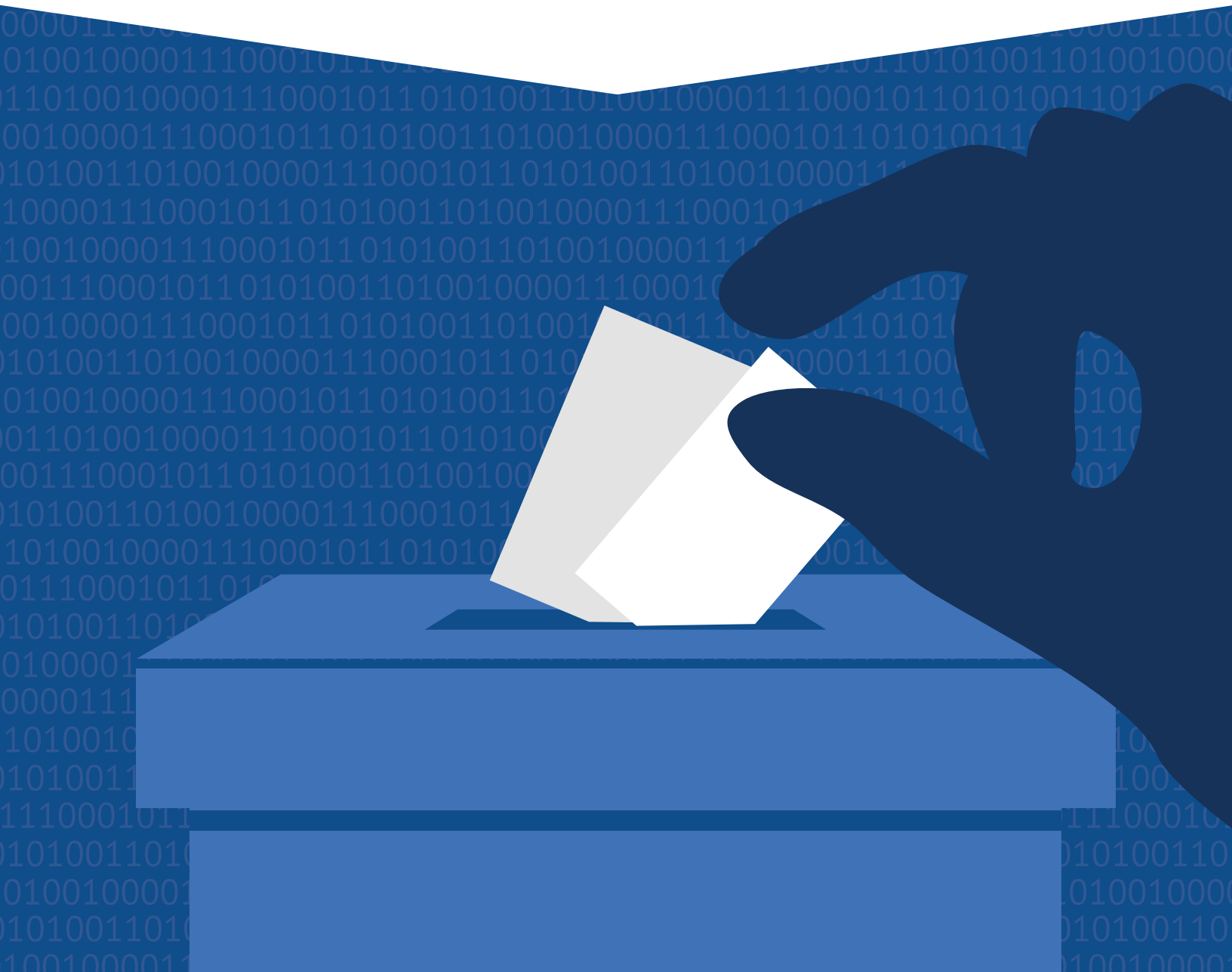
Carbon Black.

Election (In)Security

As allegations of foreign interference continue to cloud the U.S. electoral process, American voters are expressing concern when it comes to potential cyberattacks leading up to the 2018 midterm elections and beyond



Timeline

United States voters have had no shortage of cybersecurity news related to elections in recent months.

Among some of the key stories:

Prior to the 2016 U.S. Presidential Election
Democratic National Committee (DNC) is hacked; WikiLeaks releases more than 60,000 hacked emails in an apparent attempt to sway voters

Nov. 17, 2016
Obama White House confirms a pre-election warning to Russia over hacking

Jan. 6, 2017
Office of the Director of National Intelligence releases a report on Russia's alleged role in influencing the U.S. election through cyberattacks

May 9, 2017
FBI director James Comey is fired

June 6, 2017
Reality Winner is charged with releasing classified NSA documents detailing how Russia had allegedly hacked a voting equipment vendor in Florida and sent spear-phishing emails to more than 100 local election officials prior to Election Day in 2016

June 13, 2017
Reports surface that Russian cyberattacks hit systems in 39 U.S. states in the months leading up to the 2016 election; Attorney General Jeff Sessions denies collusion between the Trump campaign and Russia.

Nov. 8, 2016
Election Day - Donald Trump is elected

Dec. 2016
Congressional leaders call for an inquiry of Russian hacking; President Obama announces sanctions against Russia

Jan. 20, 2017
Donald Trump inaugurated as the 45th President of the United States

June 1, 2017
Russia's president Vladimir Putin says cyberattacks may have been the work of private Russian citizens

June 8, 2017
Former FBI Director James Comey testifies on Capitol Hill in front of the Senate Intelligence Committee

June 19, 2017
A misconfigured database containing the sensitive voting information of nearly 200 million U.S. voters was exposed on the internet by a Republican National Committee (RNC) contractor.

Executive Summary

To gauge voters' sentiment regarding election cybersecurity, how their perception has changed since the 2016 election, and how that perception may influence future voting patterns, Carbon Black recently conducted a nationwide survey of 5,000 eligible U.S. voters.

Among some of the highlights from the survey:

1. **45%** of voters said they believe the 2018 midterm elections will be influenced by cyberattacks

2. **27%** of voters said they will consider not voting in upcoming elections given their concerns about cybersecurity, **meaning as many as 58.8 million voters may stay home during future elections**

3. **45%** of voters said they trust their states and voting districts to keep their voting information safe

4. **44%** of voters believe Russia "will be back" to influence future U.S. elections, as noted in James Comey's Capitol Hill testimony

5. **54%** of U.S. voters said election cybersecurity is less secure than they thought prior to the 2016 election

6. **47%** of U.S. voters said they believe the 2016 U.S. election was influenced by foreign entities

7. Russia **45%**, The United States **20%**, North Korea **17%**, China **11%** and Iran **4%** pose the biggest risk to U.S. elections, according to voters

8. **54%** of voters said the recent NSA leaks negatively impacted their trust in the U.S. election system to keep data safe

Voter Sentiment Regarding Election Cybersecurity

Leading up to, during, and following the 2016 U.S. Presidential Election, cybersecurity was a top-of-mind issue for many voters. Prior to the election, Carbon Black conducted a survey to determine how cybersecurity fears might influence voting patterns. At the time, more than half of U.S. voters (56%) expressed concern the election would be affected by cyberattacks.

That concern appears to have carried over into 2017 as voters consider what lies ahead for the country. As we inch closer to the 2018 midterm elections, voters remain concerned that cyberattacks will influence the electoral process.

In our most recent survey (June 2017) 54% of U.S. voters said election cybersecurity is less secure than they thought prior to the 2016 election. This is translating to some anxiety as it relates to the 2018 midterm elections.

When 5,000 eligible voters were asked: "Do you believe the 2018 U.S. midterm elections will be influenced by cyberattacks?" 45% said yes, 24% said no, and 32% said they are not sure.

54% of U.S. voters said election cybersecurity is less secure than they thought prior to the 2016 election

Carbon Black.

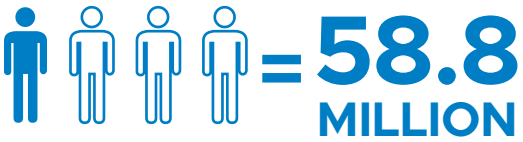
45% of U.S. voters said they believe the 2018 midterm elections will be influenced by cyberattacks

Carbon Black.

1 in 4 Voters May Not Vote in Future Elections Over Cybersecurity Concerns

In perhaps the most startling revelation from the survey, 1 in 4 voters said they will consider not voting in upcoming elections over cybersecurity fears. **Extrapolated to account for all eligible voters in the United States (about 218 million people), this means as many as 58.8 million voters may actively decide to stay home during upcoming elections, including the 2018 midterms.**

Not only is this number concerning when viewed on its own, the trend has become increasingly more alarming. When Carbon Black asked a similar question of voters prior to the 2016 election, 1 in 5 voters said they would consider not voting. T**he data is trending toward a lower level of confidence in the election process.**



1 in 4 voters said they will consider not voting in future elections over cybersecurity fears

Carbon Black.

Do Voters Trust that Data Can Be Kept Safe?

Potential voter inaction may be closely tied to voters' distrust in election authorities to keep their voting information safe. When asked: "Do you trust your state to keep your voting information safe?" and "Do you trust your voting district to keep your voting information safe?" only 45% of respondents replied "yes."

Results to this question may have been influenced by recent news. On the day this survey was conducted, it was revealed that nearly 200 million voter records were exposed on the internet when a misconfigured database used by a Republican National Committee (RNC) was discovered.

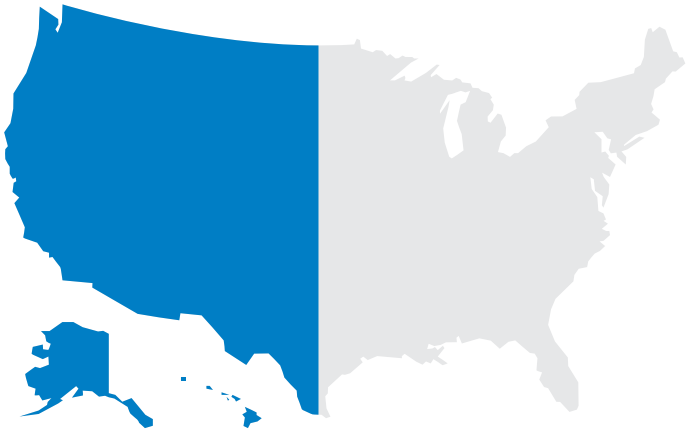
Additionally, recent reports have noted that up to 39 U.S. states had their electoral systems hit by an alleged Russian-led cyberattack.

45% of voters trust their states and voting districts to keep their voting information safe

Carbon Black.

Voter Perception on Election Influence

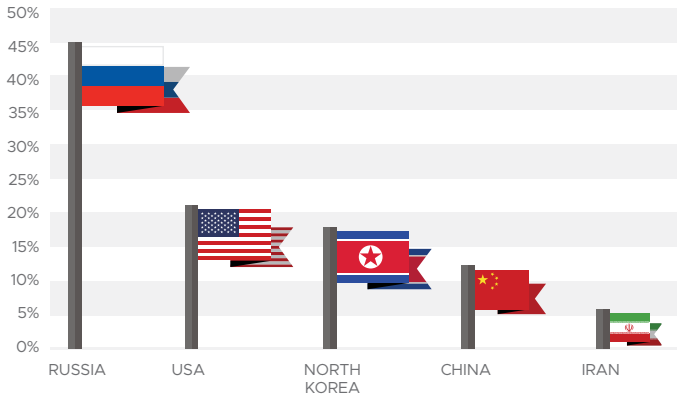
Russia's potential influence in the 2016 election has been a hot-button topic from prior to Election Day in 2016 through the present day. When asked: "Do you believe foreign entities influenced the 2016 U.S. presidential election?" nearly half (47%) of voters said yes.



47% of voters said they believe the 2016 U.S. election was influenced by foreign entities

Carbon Black.

When asked "What country poses the biggest cybersecurity risk to U.S. elections?" 45% of voters said Russia; 20% said the United States itself; 17% said North Korea; 11% said China; and 4% said Iran. (3% answered "other.")



45% of voters said they believe Russia poses the biggest cybersecurity risk to U.S. elections

Carbon Black.

While the association of election hacking to Russia appears obvious, it is interesting to note the 20% who answered "the United States." These respondents may have been influenced by the high-profile insider leaks that have made mainstream news in recent months - most notably the revelation by Reality Winner, a former NSA contractor who leaked classified documents to the media alleging how Russia hacked a voting equipment vendor in Florida and sent spear-phishing emails to more than 100 local election officials prior to Election Day in 2016.

54% of voters said the NSA leaks negatively impacted their trust in the U.S. election system to keep data safe

Carbon Black.

Will Russia "Be Back?"

As part of James Comey's testimony to the Senate Intelligence Committee in June 2017, the former FBI director noted: *"It's not a Republican thing or Democratic thing — it really is an American thing. They're going to come for whatever party they choose to try and work on behalf of. And they're not devoted to either, in my experience. They're just about their own advantage. And they will be back."*

In our survey, we asked if voters agreed with Comey's sentiment. Just fewer than half (44%) of voters said they believe Russia will attempt to influence future U.S. elections via cyberattacks.

44% of voters said they believe Russia will "Be back" to influence future elections

Carbon Black.

Looking Forward to the 2018 Midterm Elections

Cyberattacks against our elections seed doubt in democracy. The idea that even a single voter is willing to forfeit their vote in fear of a cyberattack is startling. The fact that 1 in 4 voters said they would be willing to do so speaks volumes about how deeply this doubt has penetrated.

The alleged cyberattacks surrounding the 2016 elections were a clarion call that foreign entities are motivated to disrupt U.S. elections. As we head to the 2018 midterms, the United States must prioritize restoring voters' confidence. Every vote matters. If cyberattacks threaten (or even suggest) that the individual voter is powerless, the fundamental principle of our democracy is undermined.

In too many instances, cybersecurity has become a footnote in what has become a highly politicized discussion. Cybersecurity is not a blue or red issue. When it comes to protecting our critical infrastructure - including our elections - there is no time for political grandstanding. Nor is there time for inaction.

Based on the surveys we conducted in 2016, and most recently in June, voters have expressed doubts in our election systems. Our democracy is at risk. The time is now for legislators, cybersecurity leaders, and election authorities to reach across their respective aisles in an effort to shore up our election infrastructure and restore voter confidence.

> ***Every vote matters. If cyberattacks threaten (or even suggest) that the individual voter is powerless, the fundamental principle of our democracy is undermined.***

Restoring Confidence via Security Measures

Leading up to the 2018 midterm elections, there are a number of efforts the U.S. can undertake to help restore voter confidence:

Implement stronger cybersecurity protection for online registration systems and voter databases

There is evidence to suggest that voter registration databases have been compromised in recent months. Districts, states, and contractors should be taking a careful look at their chain-of-custody policies on Election Day, as well as the security technologies in place to keep voter data protected throughout the year.

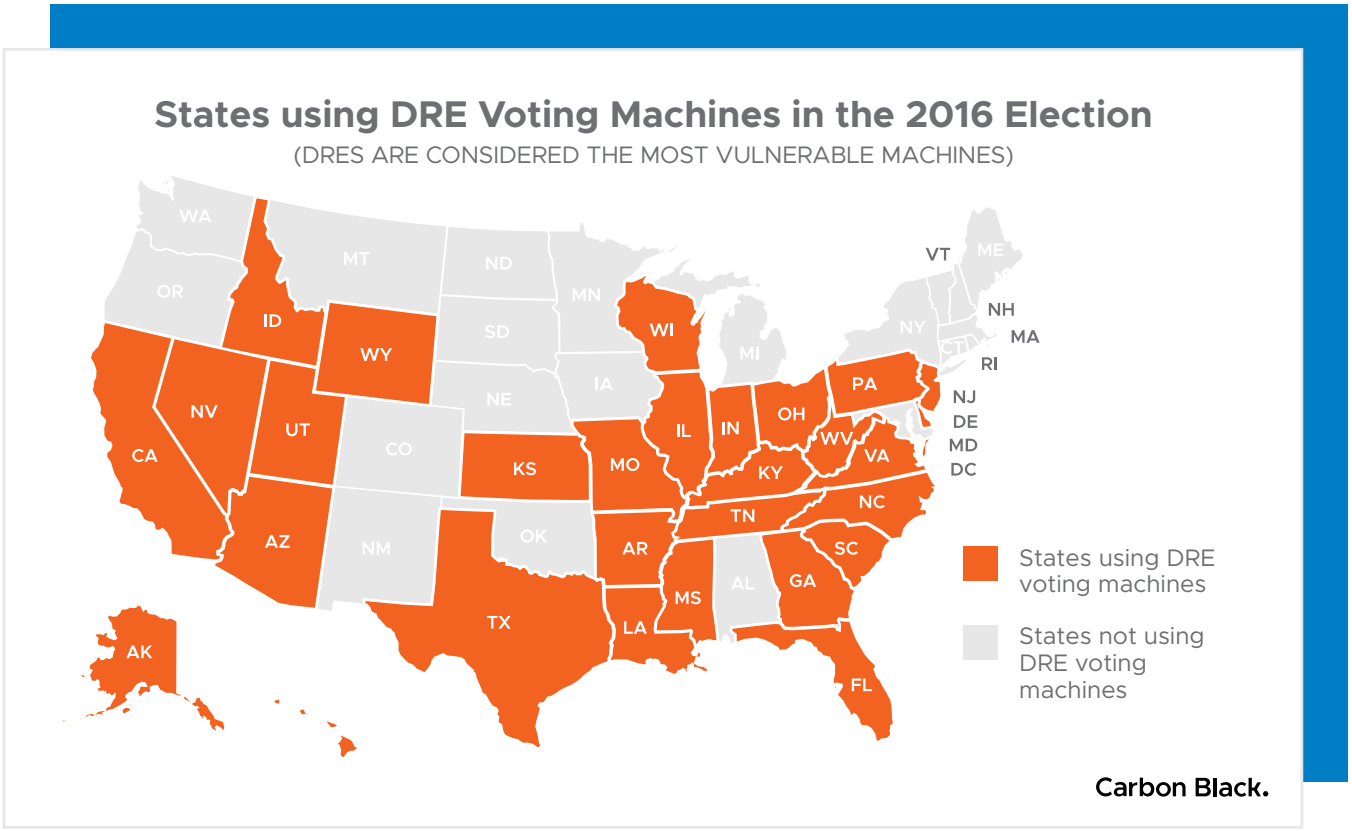
Additionally, a number of states have implemented electronic poll books where election officials can verify that a voter is registered and eligible to vote. If these electronic systems are not safeguarded by the proper cybersecurity protection mechanisms, attackers can access (and even change) voting data.

Limit (or discontinue) the use of electronic voting machines

In 2016, about 25% of the United States voted via electronic voting machines. Various types and brands of electronic voting machines were used. The type of machine considered to be the most vulnerable to attack is the "direct-recording electronic" (DRE) machine. Many of these machines are running severely outdated operated systems and the use of these machines has, for the last decade, been a divisive issue in the United States. Specific vulnerabilities on these machines have been public for years.

To date, there are no indications that technology in previous elections has been tampered with when it comes to altering or deleting votes. That's certainly good news. However, in the wake of these concerns, and recent hacks against various election entities, it is becoming clear that tampering with an election is a very real possibility. That potential for tampering, and overall doubts about election security, may play a role in keeping voters home during the 2018 midterm elections. Reliance on electronic voting machines creates an unnecessary vulnerability in our election process.

The map below from Verified Voting, a group dedicated to improving election-system integrity, shows which states use DREs.



Create an auditable paper trail of votes in every state and precinct

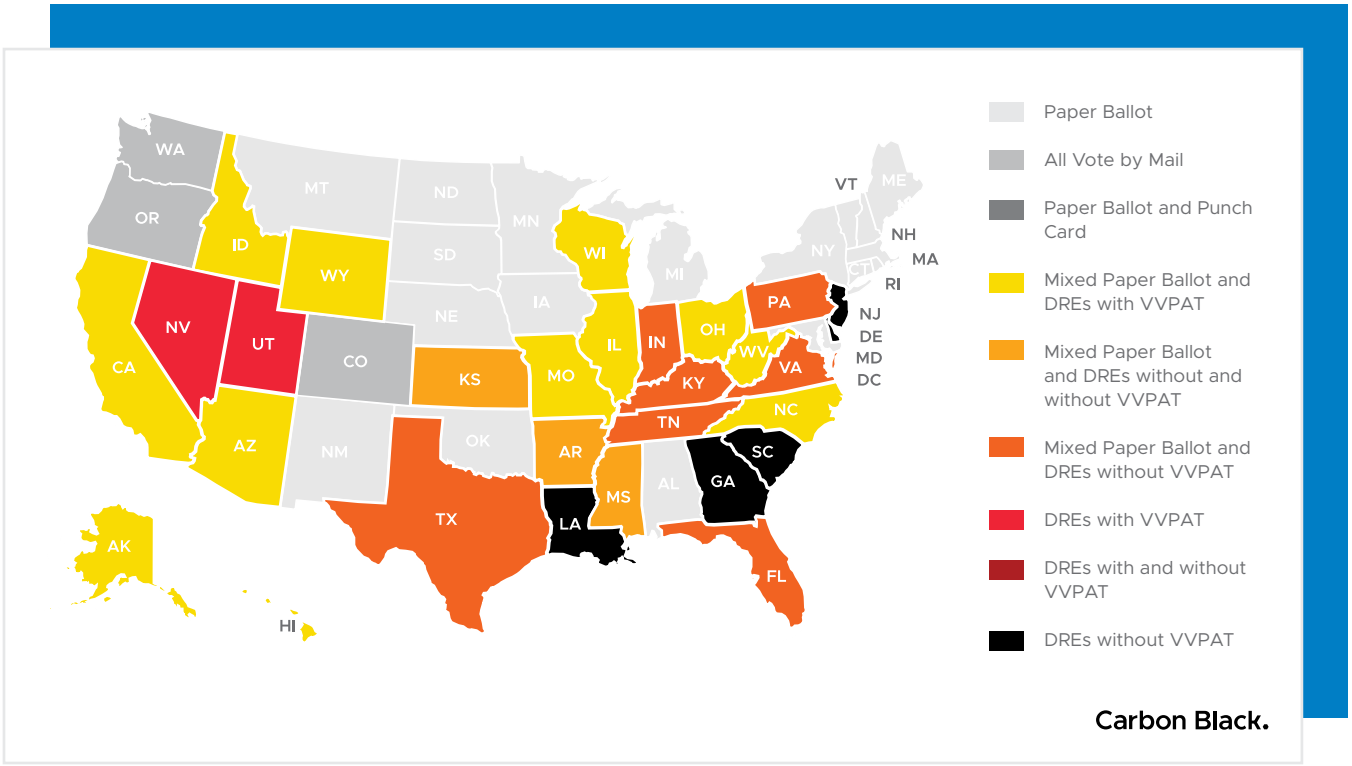
With a little more than a year until the 2018 midterms, a global policy revision regarding the usage of electronic voting machines may not be feasible without a herculean and bipartisan legislative effort. To that end, states and voting districts should work tirelessly to create an auditable system via a paper trail.

As Voter Verified notes: "The most important aspect of a voting system, with respect to accuracy, integrity and security, is whether or not it is independently auditable. That is, the very prerequisite to accuracy, integrity and security in today's voting technology is that there be a voter-marked paper ballot, or at least a voter-verifiable paper audit trail (VVPAT), for every vote cast. This ensures that election officials will have something they can use to confirm whether or not the electronic tallies produced by the voting system accurately reflected the intention of the voters."

There are several states in the U.S. using electronic voting machines without a verifiable paper trail. One such state is Georgia, which recently held a special election for its Sixth District House of Representatives seat.

The map below from Voter Verified details which states are most "at risk" when it comes to a VVPAT policies. According to Voter Verified, "16 states use DRE voting machines without a software independent voter-verifiable paper record as the standard polling place equipment in some or all counties. In these states, there is a risk that vote totals could be corrupted or lost, disenfranchising voters."

A verifiable paper trail is a critical element to restoring voters' confidence in a fair election.



Prohibit online voting

Sending in electronic votes is reserved for voters who fall under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). Thirty-one states and the District of Columbia currently allow such voting.

Cybersecurity experts overwhelmingly discourage this practice and recommend that overseas voters must return ballots via postal mail, following the 18 states that prohibit the electronic transfer of votes.

Currently, the states prohibiting electronic vote transmission are: Arkansas, Connecticut, Georgia, Illinois, Kentucky, Maryland, Michigan, Minnesota, New Hampshire, New York, Ohio, Pennsylvania, South Dakota, Tennessee, Vermont, Virginia, Wisconsin and Wyoming.

Provide additional resources so states and voting districts can better safeguard elections as critical infrastructure

In January 2017, then U.S. Homeland Security Secretary Jeh Johnson said that U.S. election infrastructure should be designated as critical infrastructure. This was, at the very least, an important step in getting the U.S. electorate to understand that cyberattacks can have real-world consequences, and that our elections are under attack.

Cyberattacks against “traditional” critical infrastructure, such as electric grids, water sources, and emergency services, can have, quite literally, life or death consequences. However, when it comes to elections, the ramifications of cyberattacks are not always as binary. Unfortunately, to date, that’s resulted in a muddied prioritization in protecting these systems.

The U.S. would be wise to take the former secretary’s designation to heart and commit the same urgency and resources to protecting its elections as it does for “traditional” critical infrastructure.

Methodology

Carbon Black conducted an online survey in June 2017 of 5,000 individuals in the United States, ages 18 and older, to determine eligible voters' sentiment regarding election cybersecurity.

The results of this survey are accurate at the 99% confidence level, representing 218,000,000 million eligible U.S. voters plus or minus a 1.8244% margin of error.

About Carbon Black

Carbon Black is the leading provider of next-generation endpoint security. With more than 9 million endpoints under management, Carbon Black has more than 3,000 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com