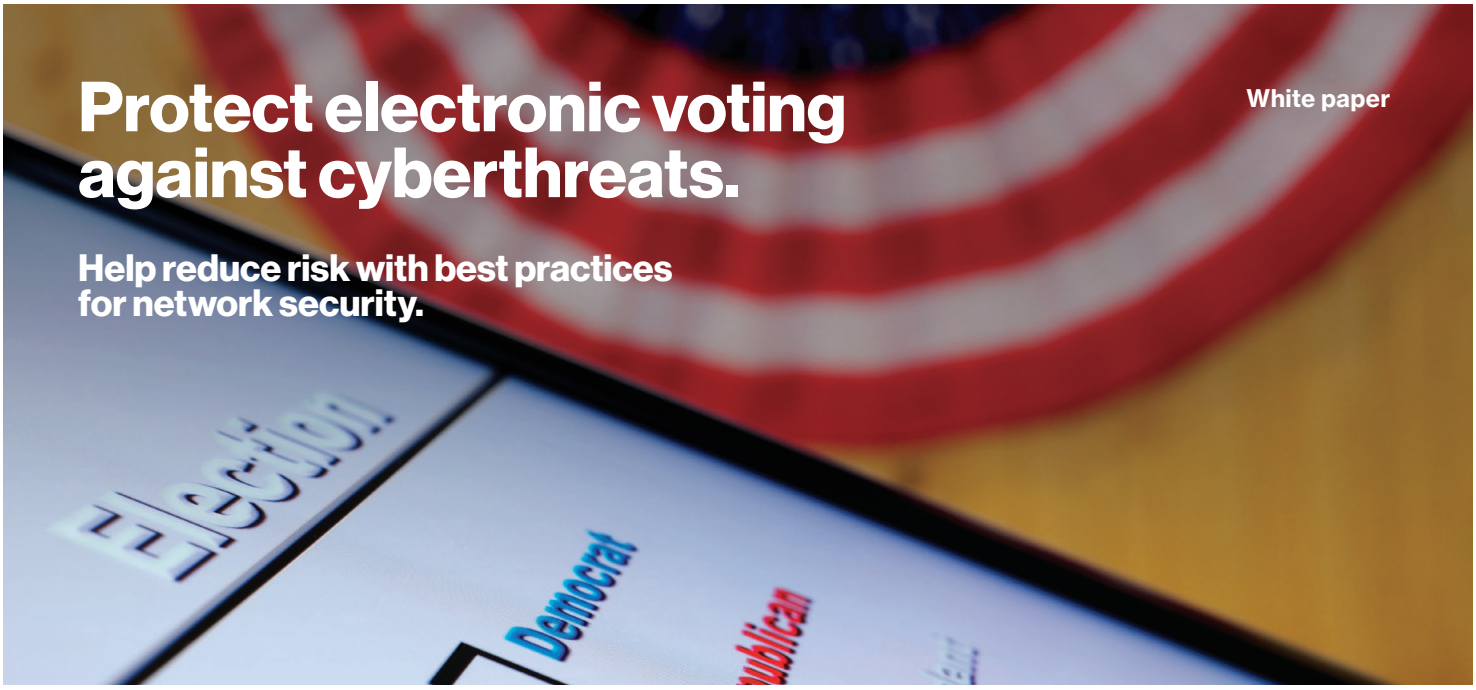
Protect electronic voting against cyberthreats.

White paper

Help reduce risk with best practices for network security.



Voter confidence in the election process rises and falls based on a mix of real and perceived risks. Real risks to elections may include domestic or foreign cyberthreats and vulnerable voting technologies. Then there are the perceived threats, which may include social media rumors and disinformation. But the lasting impression on the general public is clear—concerns about voting continue to rise. In fact, as of April, 2020, an average of only 59% of US citizens (75% Republican, 43% Democrat) believe that the 2020 November elections will be conducted fairly and accurately[1]. The approaches explored here, focused primarily on networking, can help strengthen security—and bolster voter confidence.

The 2000 presidential election, considered one of the closest elections in U.S. history[2], was a watershed event that shook voter confidence, thanks, in part, to its high-profile technical difficulties (the legendary hanging chads). Since then, voting technology has evolved, but concerns and risks remain. Cyberthreats, domestic and international, have become more pervasive and visible. News reports and documentaries focus on the many flaws in the inherently fragmented U.S. election system[3]. And heated debate continues about the best method of holding elections, from paper ballots to electronic voting, to online voting.

Election technologies, as well as levels of readiness and security, vary from state to state. But one fact crosses all state lines—election integrity and security remain hot-button issues and top priorities.

Defining the types of voting

In any discussion of voting and security, it's important to define the main approaches to holding elections and to know the real and perceived risks of each, since some of the terms can be misunderstood or used inaccurately.

Paper ballots
Voters mark a paper ballot by hand. Real and perceived vulnerabilities in voting technology have rekindled interest in this age-old approach to voting. Though simple, this approach raises issues of human error while marking and counting ballots. After voting is complete, there are several ways that ballots can be counted, including being physically scanned or otherwise compiled in a usable electronic format.

Electronic voting
Voters use an electronic voting machine to vote in person at the polls. There are many types of electronic voting machines in use at the local and state level, each with different capabilities, levels of sophistication, and methods of ensuring integrity and security. The more sophisticated versions of these voting machines are able to process both electronic and paper ballots while retaining scanned versions of both in their memory.

Online voting
Citizens vote remotely using a mobile device, eliminating the need to vote on-site or by mail. Several states have started to explore this relatively new form of voting, particularly as a method of meeting the needs of voters with disabilities and overseas voters.[4]

Vote by mail (VBM)
Exactly like it sounds, this method involves voters completing and mailing a paper ballot. While often used for special voter categories (e.g., expatriates or voters currently living outside their home states), this low-tech option has gained prominence during the COVID-19 pandemic, when in-person voting of any variety might expose voters to health risks.

verizon

Upgrading in-person voting to respond to security concerns

Though the specific solutions vary, in-person voting remains a staple of voting in the United States. Overall, it's less costly than moving to VBM[5] and more reliable and accepted than online voting, which is still in its early days. It provides broad access to all voters—including voters who need language assistance, voters with diverse circumstances (e.g., homestead mobility), and citizens who were unable to register to vote until Election Day. That said, the system is far from perfect—making security all the more important.

Recommended approaches for reducing cyberthreats—and reassuring voters

Voters may lose faith in the integrity of the vote if security risks aren't identified and mitigated. They may even choose to stay away from the polls on Election Day, lowering voter turnout. Many municipalities and states have responded to security concerns by taking a careful look at their current electronic voting systems and making significant changes and upgrades, from upgrading voting technologies to implementing more transparent (and verifiable) election processes.

During a time of intense scrutiny of voting technologies, municipalities and states have implemented these approaches to help reduce security risks. Here are just a few ways to enhance voting security and confidence at a critical juncture, when results and other key data are communicated via a network.

Keep data and devices off the public internet.
The internet is the predominant entry point for domestic and foreign cyberthreats, and election equipment can be particularly vulnerable to attacks—such as Distributed Denial of Service (DDoS) and unauthorized users attempting to gain access. As a recent Department of Homeland Security (DHS) memo pointed out, internet-connected voting is risky since ballots returned online "could be manipulated at scale" by a malicious attacker.[6] To address this risk, many municipalities and states are choosing appropriate networking solutions, such as a private wireless network, that keep their data and traffic off the internet, eliminating many vulnerabilities.

Upgrade key components.
To achieve a higher level of security, municipalities and states are adopting many of the security advances implemented by private enterprises. In many cases, boosting security means upgrading their existing electronic voting infrastructure to newer, more secure technologies that protect data and devices from attack. For example, if a city uses 3G-enabled modems, upgrading to advanced 4G LTE modems for Election Day could help improve security and reliability, since 4G LTE has improved end-to-end encryption and bandwidth capacity over 3G.

Minimize data transmission for voting machines on Election Day.
Not only is it important to keep election data and devices off the public internet, it is also important to ensure that when it comes time to transmit that data on the private network, transmission times are kept to a minimum. One way to accomplish this (though certainly not the only way) is to physically turn off any connectivity on the voting machines until after the polls have closed, at which point votes can be transmitted in a matter of minutes, given a robust network infrastructure.

Sanitize decommissioned elections equipment.
Upgrading the voting infrastructure can mean adopting new equipment. Older equipment is often discarded or resold to recyclers. To support the confidentiality and integrity of future elections, it's important to remove all information stored in all decommissioned election equipment. Municipalities and states can establish a consistent and repeatable process of cleansing the information, following the recommendations of the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST). After all, this legacy data creates both real and perceived risks. The real risk is that it will fall into the wrong hands, creating a security threat. And the perceived risk? A news story about election data discovered on a decommissioned hard drive—even if it's an anomaly—might go viral, shaping voter perceptions and shaking their confidence.

Explore and adopt proven security methods.
NIST and the EAC provide extensive guidance about election security, which could help municipalities and states upgrade their election infrastructures and help them follow solid practices in all areas of the elections process.

Adopting proven practices for network security could help address real security risks by reducing vulnerabilities and strengthening defenses. These objective security practices could even help allay perceived threats to elections—possibly reducing or eliminating them over time.

Learn more.

Contact us to learn more about how to make your elections secure.

info.verizonenterprise.com/contact_me_election

[1] Pew Research Center, national survey of U.S. adults conducted April 7-12, 2020. Source: https://www.pewresearch.org/politics/2020/04/28/two-thirds-of-americans-expect-presidential-election-will-be-disrupted-by-covid-19/

[2] Source: https://www.britannica.com/list/5-remarkably-close-us-presidential-elections

[3] Including *Kill Chain: The Cyber War on America's Elections.* Source: https://www.hbo.com/documentaries/kill-chain-the-cyber-war-on-americas-elections

[4] Source: https://www.npr.org/2020/04/28/844581667/states-expand-internet-voting-experiments-amid-pandemic-raising-security-fears

[5] Source: https://www.brennancenter.org/our-work/research-reports/estimated-costs-covid-19-election-resiliency-measures

[6] *Cyberscoop,* May 11, 2020, "DHS memo: 'Significant' security risks presented by online voting." Source: https://www.cyberscoop.com/dhs-cisa-online-voting-risks

verizon