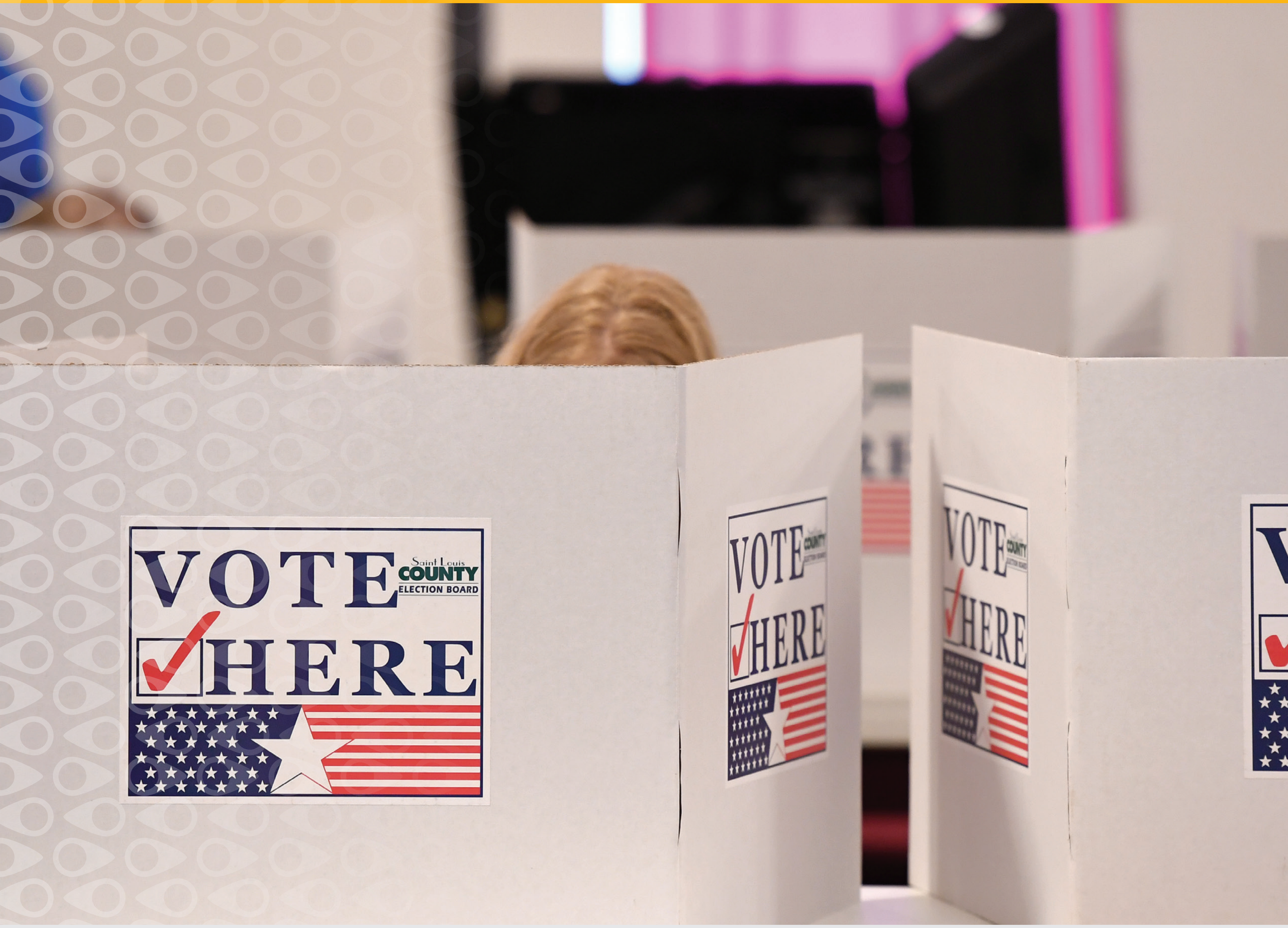
WHITE PAPER

ELECTIONS

STATE OFFICIALS MUST REASSURE VOTERS THAT ELECTIONS WILL BE PROTECTED



CYBERSCOUT®

1

VOTING SECURITY IS VITAL. IF AMERICANS CAN'T RELY ON THE METHODS AND SYSTEMS THEY USE TO CAST BALLOTS, THEY ARE IN DANGER OF LOSING TRUST AND FAITH IN PUBLIC OFFICIALS AND DEMOCRACY ITSELF.

INTRODUCTION

While the debate about Russian interference in the 2016 U.S. elections still rages, officials at the state level face a much more daunting challenge: assuring citizens that their votes in future elections will be honored and respected.

The threat that some entity—whether it's a domestic hacker, a garden-variety identity thief motivated by profit, or a nefarious state actor—will infiltrate state elections systems and attempt to undermine the 2018 elections and beyond is very real. Former FBI Director James Comey told the Senate Intelligence Committee in June that the Russians "will be back," irrespective of political party.[1] We also know that many components of the nation's patchwork system—including voter registration rolls, servers and even the voting machines themselves—have proven vulnerable to manipulation.

Experts agree that the decentralized nature of the U.S. system makes a widespread, coordinated assault on an election unlikely. But democracy relies on trust among the populace that their votes will be counted fairly and accurately. Erosion of that trust will cause citizens to lose faith in public officials at every level.

Many states are preemptively trying to forestall the inevitable next wave of attacks. There are several measures secretaries of state and elections boards can undertake to protect their states. But first it's necessary to grasp the extent of the problem.

UNDERSTANDING THE THREAT

2016: A system tested

Even before Russian efforts to affect the last national election,[2] stealing emails from the Democratic National Committee and Hillary Clinton's campaign chairman, the alarm was sounded about the country's outdated system of casting ballots. In 2015, the Brennan Center for Justice at the New York University School of Law published a report stating 43 states were using voting machines that were at least a decade old, predating Facebook.[3] Fourteen states used machines that were at least 15 years old.

No definitive proof has been found that Russian hackers were able to change any votes during the 2016 elections or alter the outcomes of any races. But there

[1] "Trump-Comey Feud Eclipses a Warning on Russia: 'They Will be Back'," The New York Times, June 10, 2017, https://www.nytimes.com/2017/06/10/us/politics/trump-comey-russia-fbi.html.

[2] "Intelligence Director Says Agencies Agree on Russian Meddling," NBC News, July 21, 2017, https://www.nbcnews.com/news/us-news/intelligence-director-says-agencies-agree-russian-meddling-n785481.

[3] "America's Voting Machines at Risk," 9, Brennan Center for Justice, 2015, http://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

IN OUR ELECTRONIC AGE, STATES' ABILITY TO PROVIDE VOTING SECURITY HAS BECOME MORE DIFFICULT. THE EXTENT TO WHICH THE ELECTORAL PROCESS CAN BE MANIPULATED IS EYE-OPENING AND DEMANDS ACTION.

were troubling signs in states around the country prior to and during the election, including these events:

- **Russian hackers gained access to a state's Board of Elections' database,** which contained the names, dates of birth, gender, driver's license numbers and partial Social Security numbers of 15 million voters. About 90,000 records were compromised. The infiltration was noticed by a part-time elections board worker who noticed unauthorized data leaving the network.[4]
- **Web security vulnerabilities were discovered in a state's voting system prior to the state's special congressional election in June.** A cyber security researcher found that the data handled by CES, which programs machines in the state, was not password-protected, and was available on a public site.[5] Days after a lawsuit was filed over the lax security, the system's servers were wiped clean.
- **Months before Election Day 2016, Russians hacked VR Systems,** the company that makes electronic "poll books"—hardware, software or a combination of both to maintain voter registration information.[6] In several cities, there were sporadic reports of problems with the machines, as people were denied at the polls, or told they were ineligible to vote.

The Intercept website described the true extent of the Russian hacking operation after it obtained a highly classified intelligence report by the National Security Agency outlining Russia's attempts to break into state elections systems.[7] In addition to VR Systems being targeted, "spear-phishing" emails were sent to more than 100 local elections officials just days before the 2016 election, The Intercept reported.

"The report indicates that Russian hacking may have penetrated further into U.S. voting systems than was previously understood. It states unequivocally in its summary statement that it was Russian military intelligence, specifically the Russian General Staff Main Intelligence Directorate, or GRU, that conducted the cyber attacks described in the document."

Subsequent reporting by Bloomberg showed that the number of states affected was 39, with one state targeted to be "Patient Zero" in a "hacking pandemic that touched four out of every five U.S. states."

[4] "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," Bloomberg Business, June 13, 2017, https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[5] "Georgia election server wiped days after lawsuit," The Hill, Oct. 26, 2017, http://thehill.com/policy/cybersecurity/357323-georgia-election-server-wiped-days-after-lawsuit.

[6] "Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny," The New York Times, Sept. 1, 2017, https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html.

[7] "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," The Intercept, June 5, 2017. https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

3

OFFICIALS AT THE STATE AND FEDERAL LEVELS CAN COUNTER ELECTION THREATS BY PUTTING PROTECTIONS IN PLACE. THESE INCLUDE COORDINATION AMONG AGENCIES, PAPER BALLOT BACKUPS, AND BETTER DEVICE CONTROL.

Machines couldn't hack it in Vegas

Hackers did what the media and elected officials could not do: reveal, in stark and stunning detail, just how flawed our voting technology really is. DEFCON, the world's longest-running and best-known hacker conference, met from July 27-30, 2017, in Las Vegas, with a record 25,000 participants gathered for the 25th annual event. Organizers created the "Voting Village," and seeded it with 30 pieces of election equipment, ranging from paperless voting machines, e-poll books, and election office networks.

"The results were sobering," according to a report based on the hackers' work and delivered to the Atlantic Council, an international affairs think tank. "By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems."[8]

GETTING PROACTIVE

How some entities are handling the threat

To prevent similar embarrassments in the future, a range of solutions have been floated, at the state and federal level:

- A bipartisan group of six U.S. senators introduced a bill called the **Secure Elections Act,** which would eliminate paperless voting machines, as well as encourage routine post-election audits.[9] Many states only conduct recounts if the margin of victory falls within a certain threshold. To help defray the cost of buying new voting technology, the bill would provide grants to states. Cost is a huge barrier for many states. In Bexar County, Texas, officials are reduced to scouring the web for old Zip disks to tabulate elections results, because the voting machines in use are no longer manufactured.[10] In Arkansas, two years ago lawmakers approved $30 million for new voting systems, but the money was never appropriated.
- In Virginia in September, two months before crucial statewide elections, including for governor, the state Board of Elections voted unanimously to decertify touch-screen voting machines, also known as Direct Recording Electronic (DRE) devices.[11] The state already had decertified AVS WinVote machines, the same ones publicly humiliated at DEFCON.

[8] "DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure," 4, DEFCON, 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

[9] "New bill could finally get rid of paperless voting machines," Ars Technica, Jan. 2, 2018, https://arstechnica.com/tech-policy/2018/01/new-bill-could-finally-get-rid-of-paperless-voting-machines/.

[10] "States scramble for funding to upgrade aging voting machines," The Associated Press, March 12, 2017, https://www.apnews.com/0bd8b3ceec964c43865c726072eb6ac8.

[11] "Virginia bars voting machines considered top hacking target," POLITICO, Sept. 8, 2017, https://www.politico.com/story/2017/09/08/virginia-election-machines-hacking-target-242492.

IN COMING MONTHS, CITIZENS WILL EXERCISE THEIR RIGHT TO VOTE. NOW IS THE TIME TO SAFEGUARD THE INTEGRITY OF THE ELECTORAL PROCESS TO ENSURE THE RESULTS ARE LEGITIMATE AND UNTARNISHED.

- Amid a nationwide return to the idea of having a paper ballot as a backup to, or replacement for, touch-screen voting, Colorado voters approved a first-of-its-kind audit that involves comparing tabulations from voting machines to a manual recount of sample ballots.[12] A number of other states are following suit with similar audits. More than 20 percent of voters nationwide in the 2016 presidential election cast ballots on machines that did not carry a verifiable paper trail.[13]

OTHER SOLUTIONS

There's an array of avenues secretaries of state and elections boards can pursue—short of asking their legislatures for more money; that's another issue entirely—to strengthen voting systems and keep the public's trust. Among them:

- **Isolate technical infrastructure** that fails a formal security audit, and insist that vendors resolve any issues.
- **Implement inventory-control processes,** to eliminate doubt that devices might have been tampered with between elections. Using barcode tape on hardware would help employees confirm a device in storage is now safe for use in the next election.
- **Limit the number of staffers** authorized to handle devices used in registration and voting.
- **Share information.** Elections are the purview of state and local officials, but federal agencies, including the Department of Homeland Security, have resources that can help.

CONCLUSION

The sanctity of the vote is as old as the American experiment in democracy. It's an issue clearly on the minds of voters from across the political spectrum. Citizens want their personal information safeguarded, and they want to ensure that elections are conducted fairly and transparently.

The 2018 elections are looming later this year. But to implement reasonable safeguards against attacks that could disenfranchise voters, bring a harsh national media spotlight, and undermine faith in democratic institutions, the clock is ticking. ■

[12] "Colorado's first-of-its-kind election audit is complete, with all participating counties passing," The Denver Post, Nov. 22, 2017, https://www.denverpost.com/2017/11/22/colorado-election-audit-complete/.

[13] "Securing the vote: How 'paper' can protect U.S. elections from foreign invaders," The Christian Science Monitor, Nov. 7, 2017, https://www.csmonitor.com/USA/Politics/2017/1107/Securing-the-vote-How-paper-can-protect-US-elections-from-foreign-invaders.