U.S. House Appropriations Subcommittee on Financial Service and General Government
"Election Security: Ensuring the Integrity of U.S. Election Systems"
February 27, 2019

Statement of Dr. J. Alex Halderman
Professor of Computer Science and Engineering, University of Michigan
Director, Michigan Center for Computer Security and Society

Chairman Quigley, Ranking Member Graves, and distinguished members, thank you for the opportunity to testify about this urgent matter of national security.

Three years ago, the United States Presidential election was attacked. Hackers penetrated political campaigns and leaked internal communications online, they manipulated social media in an effort order to sow discord, and they targeted our election infrastructure, including voter registration systems in at least 18 states. These attacks were about more than undermining voter confidence. In the assessment of the Director of National Intelligence, they marked a "significant escalation" of foreign "efforts to undermine the U.S.-led liberal democratic order".[1]

After two years of investigation by Congress and the intelligence community, we know that the attackers had the capability to do even more damage than they did. The Senate Select Committee on Intelligence has concluded that in some states, attackers "were in a position to, at a minimum, alter or delete voter registration data."[2] Had they done so (and had it gone undetected), there would have been widespread chaos on Election Day, as voters across the vulnerable states showed up to the polls only to be told they weren't registered. We were spared such a blow to the foundations of American democracy only because Russia chose not to pull the trigger.

Next time, things could be much worse, and it's not just voter registration systems that are at risk: the nation's voting machines are stunningly vulnerable to attacks that could sabotage the voting process or even invisibly alter tallies and change election outcomes. I know because I have developed such attacks myself as part of over a decade of research into election security threats and defenses.[3] Last fall, Chairman Quigley and Representative Katko invited me to demonstrate such an attack at a briefing on Capitol Hill. I brought a touch-screen voting machine used in 18 states, and we held a small mock election. I remotely hacked the voting machine to steal both Congressmen's votes and changed the election winner.[4]

---

[1] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections", January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf
[2] U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations", 2018. https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf
[3] My curriculum vitae and research publications are available online at https://alexhalderman.com.
[4] I demonstrated a similar attack for *The New York Times*, as shown in this video: https://www.nytimes.com/video/opinion/100000005790489/i-hacked-an-election-so-can-the-russians.html

This level of vulnerability is endemic throughout our election system. Cybersecurity experts have studied a wide range of U.S. voting machines, and in every case, we've found problems that would allow attackers to sabotage machines and alter vote tallies.[5]

Some people think that the decentralized nature of the U.S. voting system and the fact that voting machines aren't directly connected to the Internet make interfering in a state or national election impossible. Unfortunately, that isn't true. Some election functions are actually quite centralized, and our election infrastructure is not as distant from the Internet as it may seem.

Before every election, voting machines and optical scanners need to be programmed with the design of the ballot, the races, and candidates. Election workers create this programming on a central computer called an election management system, then transfer it to voting machines using USB sticks or memory cards. Hackers who compromise an election management system can hijack the ballot programming process to spread a voter-stealing attack to large numbers of machines.

Election management systems are often not adequately protected, and they are not always properly isolated from the Internet. Moreover, a small number of election technology vendors and support contractors program and operate election management systems used by many local governments. The largest of these services over 2000 jurisdictions spread across 34 states. Attackers could target one or a few of these companies and spread an attack to election equipment that serves millions of voters.

Furthermore, in close elections, decentralization can work against us. An attacker can probe the most important swing states or swing districts for vulnerabilities, find the areas that have the weakest protection, and strike there. In a close election, changing a few votes may be enough to tip the result, and attackers can choose where—and on which equipment—to steal those votes.

Fortunately, we know how to better defend election infrastructure and protect it from cyberattacks in 2020 and beyond. There are three essential measures:

1. First, we need to replace obsolete and vulnerable voting equipment, such as paperless systems, with optical scanners and paper ballots—a technology that 30 states already use statewide. Paper ballots provide a resilient physical record of the vote that simply can't be compromised by a cyberattack.

2. Second, we need to consistently check that our election results are accurate, by inspecting enough paper ballots to tell whether the computer results from the optical scanners are right. This can be done with what's known as a risk-limiting audit (RLA). Such audits are a common-sense quality control. By manually checking a random sample of the ballots, officials can quickly and affordably provide high assurance that the election outcome is correct.

[5] For an accessible introduction to election cybersecurity, see my online course, *Securing Digital Democracy*, which is available for free on Coursera: https://www.coursera.org/learn/digital-democracy.

3. Lastly, we need to raise the bar for attacks of all sorts—including both vote tampering and sabotage—by applying cybersecurity best practices to the design of voting equipment and registration systems and to the operation of computer systems at election offices.

These are not simply my recommendations.[6] Paper ballots, manual audits, and security best practices are a prescription endorsed by the overwhelming majority of election security experts, and by the National Academies of Science, Engineering, and Medicine.[7,8] These measures are also widely favored by election officials.

Many states have begun to implement these improvements using the $380 million in election cybersecurity funding that Congress appropriated last year. According to the Election Assistance Commission, states intend to use 36% of this funding ($136 million) for cybersecurity improvements, 28% ($103 million) for purchasing new voting equipment, and 6% ($21 million) for improving election audits.[9] These are necessary, appropriate, and urgent priorities.

However, much more needs to be done before Americans go to the polls in 2020. Although some states have made significant progress towards securing their election infrastructure, other have barely gotten started, and the nation as whole remains a patchwork of strength and weakness.

In 2018, 41 states used voting machines that were at least a decade old, and some, including parts of Pennsylvania and New Jersey, used machines dating from around 1990. Forty-three states used machines that are no longer manufactured, forcing election officials to cannibalize old machines for spare parts or even turn to eBay. Twelve states[10] still make widespread use of paperless direct-recording electronic (DRE) voting machines, which are impossible to reliably audit to detect potential errors or malfeasance. All of Georgia, for example, voted in November using the same model of vulnerable paperless DRE that I hacked in front of Chairman Quigley last fall. After years of underinvestment, America's election infrastructure is crumbling, and the $380 million can only serve as a down payment towards fixing it.

Many states would like to replace vulnerable and obsolete voting equipment before 2020, but they are struggling to figure out how to pay for it. Pennsylvania, for instance, plans to switch from insecure paperless machines to paper ballots, but the state's share of last year's HAVA

---

[6] President Trump himself has consistently endorsed the use of paper ballots, both as a candidate and since taking office. He made the point well in 2016: "There's something really nice about the old paper-ballot system. You don't worry about hacking." http://www.businessinsider.com/donald-trump-election-day-fox-news-2016-11

[7] National Academies of Science, Engineering, and Medicine, "Securing the Vote: Protecting American Democracy", 2018. https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

[8] Additionally, the National Institute of Standards and Technology (NIST) has concluded that it is not possible to effectively audit a voting system to detect and correct potential hacking without a voter-verified paper ballot.

[9] U.S. Election Assistance Commission, "EAC Releases 48 HAVA Grants State Plans, Budgets," August 2018. https://www.eac.gov/news/2018/08/21/state--territories-plan-to-spend-majority-of-hava-grant-funds-on-election-security-system-upgrades/

[10] The twelve states with large numbers of paperless DRE voting machines are: Delaware, Georgia, Indiana, Kansas, Kentucky, Louisiana, Mississippi, New Jersey, Pennsylvania, South Carolina, Tennessee, and Texas. Eight additional states use DREs with a voter-verifiable paper audit trail (VVPAT), an obsolete kind of paper backup: Arkansas, California, Illinois, Ohio, North Carolina, Utah, West Virginia, and Wyoming. Verified Voting maintains an online database of the equipment in use in each locality: https://www.verifiedvoting.org/verifier/.

funds was $13.5 million, only about 25% of the cost of implementing hand-marked paper ballots across the state. Georgia's share was $10.3 million, less than a third of what it needs just to replace its paperless machines. Without further federal assistance, we risk that new equipment and other critical improvements won't be in place for many years. With the 2020 election on the horizon—the next major target for foreign cyberattacks—we need to act before it's too late.

What will it cost to fix the problem? The highest priority should be to replace DRE voting equipment nationwide with robustly auditable paper ballots.[11] This would cost about $370 million, assuming an average of $7500 per precinct to acquire one ballot scanner and one accessible voting device.[12] Under HAVA, funds are allocated to states mainly in proportion to voting-age population, rather than by type of existing equipment. If future funding were provided under the existing HAVA formula, I estimate that about $900 million in further appropriations would be needed to ensure that every state with DREs received at least 50% of the funds needed to replace them with hand-marked paper ballots and accessibility devices.

It's important to understand that states can choose from several kinds of voting equipment, and that these choices greatly affect the overall cost and the security achieved. Fortunately, the most cost effective approach is also the most secure: hand-marked paper ballots counted using optical scanners.[13] Some localities are opting instead to purchase ballot-marking devices (BMDs), touchscreen computers that voters use to mark and print their ballots. Equipping a precinct with BMDs for all voters costs about three times as much as using hand-marked paper ballots and providing a dedicated accessibility device for voters with disabilities, and it's also less robust to cyberattacks that render the equipment inoperable. Moreover, it has yet to be established whether voters can reliably detect errors on BMD-printed ballots—which means that fraud could go undetected if the BMDs are hacked to cause them to sometimes print the wrong selections.

In many states, there are no rules in place to prevent local governments from spending federal funds on insecure and unauditable kinds of voting equipment. Some voting machine vendors continue to market paperless DREs, as well as DREs with so-called "voter-verifiable paper audit trails" (VVPATs)—a roll of paper behind a pane of glass that briefly shows the voter's selections. VVPATs are badly inferior to paper ballots, because the printouts are difficult for voters to read and challenging for election officials to effectively audit. Localities purchasing new DREs, whether or not they are equipped with VVPATs, will make it more difficult for states to implement risk-limiting audits statewide. To ensure that taxpayer money is well spent, Congress should prohibit federal funds from being used to purchase voting equipment that does not provide a robustly auditable paper ballot.

---

[11] Once paper ballots are in place, other vital security measures, such as performing risk-limiting audits, are relatively inexpensive to implement. I estimate that performing risk-limiting audits in all federal races nationally would cost less than $25 million per year on average.

[12] For additional cost estimate data, see: Brennan Center and Verified Voting, "Federal Funds for Election Security: Will They Cover the Cost of Voter Marked Paper Ballots?", March 2018. https://www.brennancenter.org/sites/default/files/analysis/Federal_ Funds_for_Election_Security_analysis.pdf

[13] Under HAVA, each polling place must also be equipped with an accessible device to assist voters with disabilities in filling out their ballots.

Election cybersecurity is an urgent matter of national security. Under our time-honored system, implementing the necessary defenses falls to states and local governments. We must not leave them to face the threat of powerful foreign adversaries unaided. Congress should provide for the common defense by equipping states with the resources they need to deploy robustly auditiable paper ballots, risk-limiting audits, and other cybersecurity improvements. With your leadership, elections in 2020 and beyond can be well secured, and voters will have good reason to have confidence in the results. But if we delay action, I fear it is only a matter of time until a national election result is disrupted or stolen in a cyberattack.