Securing Election Infrastructure with Hand-Marked Paper Ballots

Varun Gupta, Joel Hypolite, Stephen Mell, Hersh Sanghvi
University of Pennsylvania, Department of Computer and Information Science, Philadelphia, PA
University of Pennsylvania, Penn Science Policy and Diplomacy Group, Philadelphia, PA

http://doi.org/10.38126/JSPG170106

Corresponding authors: vgup@cis.upenn.edu, jhypolit@cis.upenn.edu, sm1@cis.upenn.edu, hsanghvi@cis.upenn.edu

Keywords: voting machines; election security; critical infrastructure; Congress; democracy

Executive Summary: American democracy is critically threatened by the use of insecure voting systems. Many existing electronic voting machines have malfunctioned during recent elections, and many are also vulnerable to hacking (Appel et al. 2019, Blaze et al. 2019, Blaze 2020). Most states have switched to secure, hand-marked paper ballots, but roughly 30% of Americans will continue to vote using vulnerable voting machines in 2020 (Cordova et al. 2019, Bajak 2020). While Congress allocated $380 million in 2018 and $425 million in 2020 to improve election security, these funds were neither targeted at nor sufficient for replacing all electronic voting machines. We propose that Congress (1) allocate $110 million exclusively for transitioning away from electronic voting machines and (2) prohibit the use of federal funds for purchasing voting systems that do not primarily use hand-marked paper ballots. This one-time transition cost is much smaller than even annual expenditures on other critical infrastructure (Copeland 2010; Halderman 2019). Replacing electronic voting machines with hand-marked paper ballots is the most affordable and secure option.

I. Statement of issue

Voting machines, integral parts of each state's election infrastructure, are universally vulnerable to malfunction, misconfiguration, and hacking (Appel et al. 2019). However, the risks posed by compromised voting machines depend on what role they play in elections (Blaze 2020).

Voting machines broadly fall into three categories:

- **direct recording electronic** (DRE) systems, wherein votes are cast and counted electronically, with no paper trail.
- **ballot marking device** (BMD) systems, wherein voters make their choices electronically and receive a marked paper ballot to be tabulated.
- **hand-marked paper ballot** (HMPB) systems, wherein voters fill out paper ballots by hand, which are then counted with optical scan readers.

Figure 1 illustrates which kind of system each county will use in 2020.

Direct recording electronic machines are the least secure of the available systems, and will be used by an estimated 16 million (about 1 in 10) American voters in 2020 (Cordova et al. 2019). Software bugs could cause these machines to silently alter votes in a way that would be impossible to detect, since these machines leave no voter-verified record. For example, a post-election statistical study showed that at one polling place during the 2018 gubernatorial election in Georgia, 14% of votes were recorded incorrectly due to a misconfigured DRE (Ottoboni et al. 2019). Similarly, in a 2019 Mississippi election, some voting machines in 7 counties would not allow voters to select certain candidates (Axelrod 2019). At least 15 Texas voters also reported that DREs flipped their votes in the 2018 Senate election, despite the manufacturer knowing of such malfunctions for over a decade (Zetter 2018).

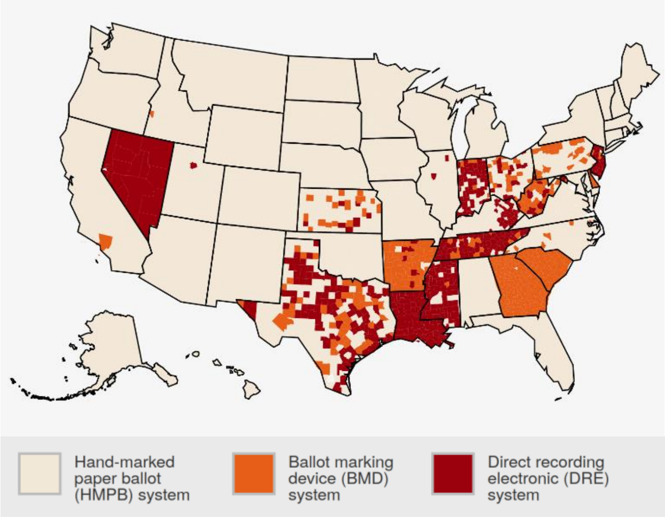
Hand-marked paper ballot (HMPB) system
Ballot marking device (BMD) system
Direct recording electronic (DRE) system

Figure 1: An estimated 30% of American voters will use insecure voting machines in 2 020. Indiana, Louisiana, Mississippi, Nevada, New Jersey, Tennessee, and Texas heavily use DREs. Arkansas, Georgia, South Carolina, and West Virginia heavily use BMDs. Adapted from Verified Voting 2020.

While there is no evidence to suggest these examples were malicious attacks rather than malfunctions, experts have cautioned that there are abundant opportunities for targeted attacks on DREs. In New Jersey, experts were able to hack voting machines in the field in under 7 minutes (Appel et al. 2009), yet those machines are still in use today (Anthes 2019). These incidents illustrate that DREs are vulnerable and could be hacked prior to or during elections. Such malicious alterations would be almost impossible to detect, and hacked DREs could have catastrophic effects on elections.

Ballot marking devices are also insecure and will be used by roughly 30 million (about 1 in 5) American voters in 2020 (Bajak 2020). Security researchers have found numerous vulnerabilities in popular BMDs used in over 20 states (Blaze et al. 2019). In one instance, the researchers found they could alter the candidate and election information stored in the machine causing printed ballots to differ from voter selections. Although BMDs produce voter-verifiable paper records, such voter-verification fails in practice. In a simulated election where every voter's ballot was modified by the BMD, only 40% of voters checked their ballots, and fewer than 7% reported the error to a poll worker (Bernhard et al. 2020). Evidence suggests that factors limiting self-verification of ballots include: voters not having a proper area to comfortably and privately verify their ballots; not knowing how to report that their ballot was marked incorrectly; and not knowing BMDs can erroneously mark ballots (Appel et al. 2019). Because only individual voters can verify that the machine-marked ballot correctly expresses their intended vote, incorrectly marked ballots cannot be discovered with risk-limiting audits or recounts.

Hand-marked paper ballot systems are not vulnerable to hacking or misconfiguration of machines in the same way. Though electronic scanning machines used to count HMPBs may fail, the ballot serves as an accurate record of voters' intentions. Therefore, auditing techniques known as 'risk-limiting audits', which use statistical techniques to sample ballots based on the margin of the election result, can be reliably used to obtain a confidence measure on the election outcome (Lynch 2019). Risk-limiting audits, which are increasingly being adopted by states that already use HMPBs, can ensure that miscounting by scanners is detected and can be corrected (Lynch 2019).

HMPB systems are also simpler for most voters to use and less expensive than electronic systems. New BMD systems in Pennsylvania cost more than twice as much as new HMPB systems (Deluzio and Skoglund 2019). Subsequently, recurring expenses are lower for paper systems, as partially or fully electronic systems have components that are expensive to operate and maintain (National Election Defense Coalition 2020). Hand-marked systems are also less prone to failures that create long lines at polling places (National Election Defense Coalition 2020).

II. Background

As understanding of the insecurities and threats regarding voting infrastructure has matured, the federal government has taken measures to address the concerns. In 2017, the Department of Homeland Security designated the U.S. election infrastructure as critical infrastructure (CI), recognizing "the vital role elections play in this country" (Jeh 2017). This designation affords the election infrastructure all the benefits and protections of CI, placing it alongside the sixteen other CI sectors, including water, power, and medical. To this end, specific federal action has focused on cybersecurity assistance and coordination, providing services to states including training, information sharing, vulnerability assessments, threat detection and hunting, and incident response

(DHS Election Security 2020). While the CI designation focuses on ensuring the existing election infrastructure is secured, it is still important that states make secure choices during procurement.

In 2018, the National Academies of Science, Engineering, and Medicine formed the Committee on the Future of Voting to document the current state of voting technology and standards, examine challenges, assess ongoing efforts to improve voting, and recommend steps that stakeholders should take to improve the security of the election infrastructure. Their study involved extensive review of background material and testimony from election administrators and experts from government, industry, and academia, including election security researchers. They recommended that all local, state, and federal elections be conducted using HMPBs, basing this recommendation on three key findings: (1) the most significant threat to the U.S. election system comes from actors who aim to undermine election results, (2) the technology to guarantee secure electronic voting against such threats simply does not exist, and (3) with current technology, HMPBs are required to obtain the physical records necessary to perform comprehensive post-election audits (National Academies of Sciences, Engineering, and Medicine 2018). This highlights the importance of targeting new legislation, since procuring insecure systems puts a strain on CI resources whose responsibility it is to provide safety and assurance.

III. Effects of the Help America Vote Act of 2002

The Help America Vote Act (HAVA) is the primary way in which Congress guides procurement of election infrastructure. Congress allocated funding under HAVA for 2018 ($380 million) and 2020 ($425 million) to broadly support election technology and security (H.R. 1625; H.R. 1158). These funds are distributed among states based on a two part formula. First, a minimum payment is determined based on a percentage of the total allocation. Second, an additional amount is determined based on the relative size of a state's voting-age population compared to all other states, as reported in the most recent decennial census. Of the 2018 funding, only 28% went to the purchase of new voting equipment (U.S. Election Assistance Commission 2018). The other 72% went towards expenses related to post-election audit activities, improving voter registration systems, cybersecurity enhancements, election-related communication efforts, and other state-specified activities. Though the 2020 funding prohibits the purchase of DRE systems, it allows the purchase of BMD systems (H.R. 1158).

IV. Policy options

We consider three policy options that Congress may undertake to bolster states' election infrastructure: maintaining the status quo of allowing the purchase of BMD systems with federal funds; restricting the use of federal funds to the purchase of HMPB systems and allocating additional funds to help states transition; and allocating funding for research and development of secure voting machines.

i. Option 1: Maintain the status quo

Congress could pass no new legislation, continuing to allow federal funds to be used to purchase BMDs.

Advantages

- This avoids one-time transition costs to overhaul voting systems.

Disadvantages

- Even BMDs that produce readable paper trails are insecure and difficult to audit (Bernhard et al. 2020).
- Under the current population-based HAVA allocation formula (see Section III), states with populations that are relatively low compared to the number of DREs to replace will not be allocated sufficient funds to replace all their highly vulnerable DREs. In 2019, it was estimated that $900 million in HAVA appropriations would be needed to replace the DRE infrastructure across all states (Halderman 2019). After accounting for the 2020 HAVA allocations, an additional $475 million in appropriations is still needed.
- BMDs and DREs often cause lines at polls when machines break (Gardner et al. 2018).

ii. Option 2: Require the use of paper ballots, except by disabled persons

Congress could pass new legislation separate from HAVA to:

- Require that voting systems purchased with federal funds use only HMPBs, except for accessible BMDs for use by people with disabilities.

- Allocate $110 million exclusively for the replacement of DRE and BMD systems based on need, determined by the number of voters that use potentially insecure machines in each state, rather than the population-based HAVA allocation formula described in Section III. This cost amount was calculated based on Halderman (2019)'s estimate for states to switch from DREs to HMPBs ($370 million), adjusted for the estimated expenditures for replacing voting machines from the 2018 ($145 million) and 2020 ($115 million) HAVA allocations (derived from Brennan Center for Justice 2018). As seen in Figure 1, this needs-based allocation would most help states that heavily rely on aging DRE and BMD-based infrastructures

Advantages

- Purchasing new HMPB systems costs half as much per voter as replacing BMDs (Deluzio and Skoglund 2019).
- HMPBs are more secure than BMDs and DREs because risk-limiting audits can be used to ensure correct election results (Lynch 2019; Appel 2019).
- HMPBs are more reliable than BMDs and DREs because machine breakages do not stop voters from casting ballots (National Academies of Sciences, Engineering, and Medicine 2018).

Disadvantages

- Incurs a one-time transition cost, but this cost is small relative to both the annual cost to secure other CI and to the total HAVA allocations so far (see Figure 2).

iii. Option 3: Invest in the development of formally verified voting machines

Recent advances in formal verification, a mature area of computer science concerned with improving the security and reliability of systems, offer optimism for the future of electronic voting machines (Fisher et al. 2017; Gu et al. 2016; Leroy et al. 2016). Formal verification uses formal methods, a family of rigorous mathematical techniques, to both specify and verify desirable program behavior.

For example, a formal specification of voting machine behavior may include several security relevant properties to ensure a voter is voting in the proper election, that once a voter casts a ballot it cannot change, etc. Proof checking software monitors the system to verify that these and other statements in the specification remain true during system operation. Because developing such formally verified software is labor-intensive, it is most common in defense and aerospace settings. Although formally verified voting machines would still be susceptible to physical tampering, formal verification could sufficiently mitigate the software defects that cause the issues described in our statement of issue and those that are exploited by the vast majority of malicious hacks (Blaze et al. 2019).

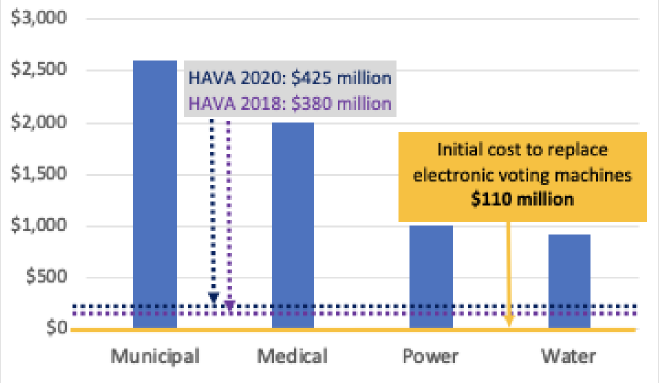

Figure 2: The one-time cost of securing elections is less than the annual cost of securing other critical infrastructure. Costs in millions of dollars. Data derived from Halderman 2019, Brennan Center for Justice 2018, Zpryme 2013, Copeland 2010, OMB 2020, and Grand View Research 2016.

Congress could pass new legislation to:

- Instruct the National Institute of Standards and Technology to define formal specifications of correctness for voting machines.
- Allocate funding for the development of such formally verified voting machines.

After such verified machines have been developed, Congress would need to allocate additional funding for the production or purchase of such machines.

Advantages

- Largely mitigates risks to election security due to software defects in voting machines.

Disadvantages

- Costly, both in research and in eventual procurement.
- Leaves status quo voting systems in place during years of research and development. Research and development of verified voting machines is not guaranteed to be successful.

V. Policy Recommendation

Congress should pursue *Option 2*, to prohibit the use of federal funds to purchase insecure voting machines and allocate money to help states transition to hand-marked paper ballot systems. Inaction would continue to leave our election systems vulnerable. Developing provably secure voting machines would require substantial time and leave our elections vulnerable in the interim, with limited additional benefit. Universally recommended by experts in election security, *Option 2* is simple and effective, the best choice for securing our democracy.

References

Anthes, Rob. 2019. "Hacked in 7 minutes: questions of vulnerability surround New Jersey's aging voting machines." Community News. Published October 31, 2019. https://communitynews.org/2019/10/31/hacked-in-7-minutes/

Appel, Andrew, Maia Ginsburg, Harri Hursti, Brian Kernighan, Christopher Richards, Gang Tan, Penny Venetis. "The New Jersey Voting-machine Lawsuit and the AVC Advantage DRE Voting Machine." USENIX Association. Published August 2009. https://www.usenix.org/legacy/events/evtwote09/tech/full_papers/appel.pdf

Appel, Andrew, Richard DeMillo, and Philip B. Stark. "Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters." *SSRN*. May 21, 2019. http://dx.doi.org/10.2139/ssrn.3375755

Axelrod, Tal. "Mississippi officials confirm multiple cases of voting machines changing votes in GOP governor runoff." The Hill. August 27, 2019. https://thehill.com/policy/cybersecurity/459067-mississippi-officials-confirm-multiple-cases-of-voting-machines-changing

Bajak, Frank. 2020. "Reliability of Pricey New Voting Machines Questioned". February 23, 2020. https://www.usnews.com/news/politics/articles/2020-02-23/reliability-of-pricey-new-voting-machines-questioned

Bernhard, Matthew, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. 2020. "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" IEEE Symposium on Security and Privacy (Oakland 2020).

Blaze, Matt, Harri Hursti, Margaret Macalpine, Mary Hanley, Jeff Moss, Rachel Wehr, Kendall Spencer, Christopher Ferris. 2019. "Def Con 27 Voting Machine Hacking Village Report." Published August 2019. https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf

Blaze, Matt. "Testimony Before the US House of Representatives Committee on House Administration - Hearing on '2020 Election Security – Perspectives from Voting System Vendors and Experts.'" January 9, 2020. https://www.mattblaze.org/papers/blaze-houseadmin-20200109.pdf

Brennan Center for Justice, Verified Voting. "Federal Funds for Election Security: Will They Cover the Costs of Voter Marked Paper Ballots." March 23, 2018. https://www.brennancenter.org/our-work/research-reports/federal-funds-election-security-will-they-cover-costs-voter-marked-paper

Gu, Ronghui, Zhong Shao, Hao Chen, Xiongnan Newman Wu, Jieung Kim, Vilhelm Sjöberg, and David Costanzo. "Certikos: An extensible architecture for building certified concurrent {OS} kernels." In 12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16), pp. 653-669. 2016.

Copeland, Claudia. 2010. "Terrorism and Security Issues Facing the Water Infrastructure Sector." CRS Report for Congress. Congressional Research Service. RL32189. December 15, 2010

Córdova, Andrea, Elizabeth Howard, and Lawrence Norden. 2019. "Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary." Brennan Center for Justice. August 13, 2019. https://www.brennancenter.org/our-work/analysis-opinion/voting-machine-security-where-we-stand-six-months-new-hampshire-primary

Deluzio, Christopher and Kevin Skoglund. "Pennsylvania Counties' New Voting Systems: An Analysis." August 15, 2019. https://www.cyber.pitt.edu/votingsystemsanalysis.

DHS Election Security. July 14, 2020. Accessed August 20, 2020. https://www.dhs.gov/topic/election-security

Fisher, Kathleen, John Launchbury, and Raymond Richards. "The HACMS program: using formal methods to eliminate exploitable bugs." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 375, no. 2104 (2017): 20150401.

FBI National Press Office. "FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure." January 16, 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-new-policy-for-notifying-state-and-local-election-officials-of-cyber-intrusions-affecting-election-infrastructure

Gardner, Amy, and Beth Reinhard. "Broken machines, rejected ballots and long lines: voting problems emerge as Americans go to the polls." November 6, 2018. Washington Post. https://www.washingtonpost.com/politics/broken-machines-rejected-ballots-and-long-lines-voting-problems-emerge-as-americans-go-to-the-polls/2018/11/06/ffd11e52-dfa8-11e8-b3f0-62607289efee_story.html

Gerwin, Klein, June Andronick, Matthew Fernandez, Ihor Kuz, Toby Murray, and Gernot Heiser. "Formally Verified Software in the Real World." Communications of the ACM Vol. 61 No. October 10, 2018. https://cacm.acm.org/magazines/2018/10/231372-formally-verified-software-in-the-real-world/abstract

Grand View Research. "Healthcare Cyber Security Market Size, Analysis Report." Published April 2016. https://www.grandviewresearch.com/industry-analysis/healthcare-cyber-security-market

Halderman, J. Alex. "Election Security: Ensuring the Integrity of U.S. Election Systems." February 27, 2019. Testimony Before Congress. https://jhalderm.com/pub/misc/fsgg-voting-written19.pdf

H.R. 1625. "Consolidated Appropriations Act, 2018." 115th Congress. March 28, 2018.

H.R. 1158. "Consolidated Appropriations Act, 2020." 116th Congress. December 20, 2019.

Johnson, Jeh. "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." Department of Homeland Security, January 6, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

Leroy, Xavier, Sandrine Blazy, Daniel Kästner, Bernhard Schommer, Markus Pister, and Christian Ferdinand. "CompCert-a formally verified optimizing compiler." 2016.

Lynch, Dylan. "Checking the Election: Risk-Limiting Audits." *National Conference of State Legislatures* 27 no. 26 (2019). https://www.ncsl.org/research/elections-and-campaigns/checking-the-election-risk-limiting-audits.aspx.

National Election Defense Coalition. 2020. "The National Election Defense Coalition Opposes Adopting Ballot Marking Devices as the Primary Method of Voting." Accessed May 2020 https://www.electiondefense.org/ballot-marking-devices.

National Academies of Sciences, Engineering, and Medicine. 2018. "Securing the Vote: Protecting American Democracy." Washington, DC. The National Academies Press, 2018. https://doi.org/10.17226/25120.

NCSL: National Conference of State Legislatures. 2018. "Voting System Standards, Testing, and Certification." Accessed August 19, 2020. https://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx

NIST: National Institute of Standards and Technology. "Voting." Accessed August 19, 2020. https://www.nist.gov/itl/voting

OMB: Office of Management and Budget. 2020. "A Budget for America's Future, Fiscal Year 2021 Budget of the U.S. Government." Executive Office of the President. Published January, 2020. Washington D.C. https://www.whitehouse.gov/wp-content/uploads/2020/02/spec_fy21.pdf

Ottoboni, Kellie and Phillip B. Stark. 2019. "Election Integrity and Electronic Voting Machines in 2018 Georgia, USA." International Joint Conference on Electronic Voting. September 24, 2019. https://doi.org/10.1007/978-3-030-30625-0_11

U.S. Election Assistance Commission. "The Impact of HAVA Funding on the 2018 Elections." Accessed May 31, 2020. https://www.eac.gov/sites/default/files/paymentgrants/TheImpactofHAVAFundingonthe2018Elections_EAC.pdf.

U.S. House of Representatives. Joint Explanatory Statement Accompanying H. R. 1158. https://docs.house.gov/billsthisweek/20191216/BILLS-116HR1158SA-JES-DIVISION-C.pdf

Verified Voting. "Policy on Direct Recording Electronic Voting Machines and Ballot Marking Devices." Accessed July 23, 2020. https://www.verifiedvoting.org/wp-content/uploads/2019/08/VV-BMD-Policy-V3-LARGE.pdf

Verified Voting. "Verifier." Accessed April 3, 2020. https://www.verifiedvoting.org/verifier

Zetter, Kim. 2018. "Texas Voting Machines Have Been 'a Known Problem' for a Decade." VICE Motherboard. October 30, 2018. https://www.vice.com/en_us/article/negayg/texas-voting-machines-have-been-a-known-problem-for-a-decade

Zpryme. 2013. "Global Smart Grid Cybersecurity Systems Market Value (2012 – 2020)." Published April 16, 2013. https://zpryme.com/reports/global-smart-grid-cybersecurity-systems-market-value-2012-2020/

Varun Gupta is a Ph.D. student in Computer Science at the University of Pennsylvania. He is interested in machine learning and technology policy.

Joel Hypolite is a Ph.D. candidate in Computer Science at the University of Pennsylvania. He received his BS in Computer Science from the University of Notre Dame. His research interests are broadly in the areas of networking, security, and artificial intelligence.

Stephen Mell is a Ph.D. student in Computer Science at the University of Pennsylvania. He received his Bachelor of Arts in Mathematics at Washington University in St. Louis. His research interests lie at intersection between computational learning and formal logic.

Hersh Sanghvi is a Ph.D. student in Computer Science at the University of Pennsylvania. He received his B.S in Electrical and Computer Engineering from the University of California, Berkeley in 2019. His research interests lie in the areas of robotic perception and control.