

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, ET AL.,
Defendants.**

**DECLARATION OF
J. ALEX HALDERMAN IN
SUPPORT OF MOTION FOR
PRELIMINARY INJUNCTION**

Civil Action No. 1:17-CV-2989-AT

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. Under the State of Georgia's planned adoption of a paper-based voting system using ballot-marking devices ("BMDs"), in-precinct optical scanners, and other components provided by the State's vendor, Dominion Voting Systems, Inc. ("Dominion"), BMDs will print barcodes on each ballot, which the optical scanners will read to interpret a voter's selections and to provide election results for all ballots scanned on each scanner (the "Proposed Election System").

3. Despite the purchase and deployment of new equipment for the Proposed Election System, important databases, files, computers, and personnel will carry forward from the current election system (the “GEMS/DRE System”). This means that vulnerabilities in these aspects of the GEMS/DRE System will also affect the security of the Proposed Election System. If attackers have already infiltrated the GEMS/DRE System, then these points of continuity could provide a foothold from which to attack elections conducted under the Proposed Election System.

4. There are several ways attackers could subvert the Proposed Election System or any other system making use of computerized or Internet-connected components, several of which I have described in my prior declarations. BMDs are computers, meaning they are susceptible to hacking and interference.

Ballot Barcodes Create Elevated Hacking Risks

5. In the Proposed Election System, the optical scanners use the barcode on the paper ballot as the exclusive means of interpreting the voter’s choices. This increases the likelihood that attackers will be able to compromise election results. Although the optical scanners themselves might be hacked as a way of producing fraudulent results, the use of barcodes makes it possible for attackers to commit difficult-to-detect fraud by hacking *either* the scanners or the BMDs. This increases

the “attack surface” of the election system: with two potentially vulnerable components to target instead of just one, attackers are more likely to succeed.

6. Under one plausible attack scenario, an attacker could infect BMDs with malicious code that causes them to print barcodes that encode votes for candidates other than the voter’s intended selections. This malicious software would leave the human-readable text of the ballot unchanged. Since voters cannot read barcodes unaided, they would be unable to detect the deviation between the text and the barcode. However, since the optical scanners ignore the human-readable text and count only the barcodes, the election results would reflect the fraudulent selections.

7. In principle, a sufficiently rigorous audit of the human-readable portion of the ballots could detect and correct such an attack. However, since attackers might choose to target any race in any election, every race and every election would need to be rigorously audited in order to rule out barcode-based fraud. Although a growing number of U.S. jurisdictions are implementing risk-limiting audits, to my knowledge no jurisdiction has announced plans to routinely perform RLAs that cover every race to high statistical confidence.

8. Moreover, Georgia law does not contemplate, let alone provide for, audits of sufficient frequency, scope, or reliability to confirm barcode-based totals. Act 24 provides only for pilots of risk-limiting audits by the end of 2021, does not

mandate their adoption if the pilots are successful, and does not apply to every race in every election. This audit regime, even if implemented, cannot detect error or fraud in races that are not audited.

9. In Dominion’s response to the State’s request for proposals, it contemplated an update to its BMDs such that they would not need to print barcodes on ballots.¹ Instead, the BMDs would produce (and the scanners would count) an entirely human-readable ballot capable of verification by the voter. However, this option is described as an “upgrade” available only after “certification is complete at the EAC.”

10. The Secretary of State’s office and Dominion portray Dominion Image Cast X BMDs as having this ability to print such a human-readable, “full-face” ballot. A video portraying such a capability is part of the “Important Voter Information” available to the public on the Secretary of State’s elections security web page.² The video portrays a voter making her selections on a BMD displaying a mock ballot using Georgia state and local races and constitutional questions or referenda. At the

¹ See “Clarification Questions\MS 16-1 Supply Chain_Dominion and KNOWiNK Final.docx” available at <https://sos.ga.gov/admin/uploads/Dominion.zip> (last visited Sept. 18, 2019).

² <https://www.dropbox.com/s/u0lc21u82ye2qpg/ICX%20BMD%20Cart.mp4>, available through “Voting Cart” hyperlink at sos.ga.gov/securevoting (last visited Sept. 19, 2019).

end of the video, the voter selects “Print Ballot,” and the attached printer produces a double-sided ballot with a darkened oval appearing next to the voter’s selections.³

11. Dominion’s in-precinct optical scanners already are capable of and certified to read such full-face paper ballots. Dominion’s contemplated update to the BMDs, if deployed, would reduce the risk of hacking owing to the use of an illegible barcode that is incapable of voter verification.

BMDs Limit the Effectiveness of Voter Verification

12. Even if the BMDs produced human-readable ballots to the exclusion of barcodes, the voter would still need to read the ballot carefully enough (and recall all of her selections well enough) to verify it. It is possible, for example, that a BMD could be maliciously programmed or otherwise malfunction such that the ballot printed by the BMD does not match the voter’s intended selections. If voters do not reliably detect when their paper ballots are wrong, no amount of post-election auditing can detect or correct the problem.

13. Collaborators and I at the University of Michigan recently ran experiments to determine how often voters fail to notice that their BMD-printed ballots differ from their on-screen selections. We set up a realistic mock polling place

³ *Id.*

at a city library and had 241 library patrons vote using BMDs and an optical scanner. My research assistants programmed the BMDs so that every printed ballot would contain one race (chosen at random) where the vote was different from the voter's selection. We recorded how many of the voters noticed the error and reported it to a poll worker or on an exit survey.

14. Our results (which are currently undergoing peer review) suggest that voters do not reliably verify BMD-printed ballots unless prompted to do so in very specific ways.⁴ When not given any prompting, only 6.5% of participants noticed that their votes had been changed by the BMD.

15. In an election with a 1% margin of victory, an attacker could change the outcome by altering as few as 0.5% of the ballots. If only 6.5% of voters whose ballots are affected notice and report the problem, then there will be one complaint for every 3000 voters, or less than one per precinct on average. This rate is so low that poll workers would be unlikely to notice that there was a systemic problem. However, both the electronic count from the optical scanners and the set of paper ballots would

⁴ We also tested a variety of possible interventions to see whether they increased the rate of voter verification. Several had no effect, including signage and variations in ballot layout. Two showed significant promise: (i) having a poll worker instruct voters approaching the scanner to carefully check their ballots, and (ii) ensuring voters started with a written slate of candidates that they could easily compare to the printed ballot. Further research and testing are necessary to establish whether interventions such as these would be effective in real elections.

reflect a fraudulent election outcome. Even if the problem were recognized, the only remedy would be to rerun the election.

16. It is true that voters using hand-marked paper ballots also make errors. However, for the most part, human errors in hand-marked paper ballots tend to be random. Errors that favor a candidate tend to be largely canceled out by errors that disfavor that candidate. This has a tendency to equalize the effect of errors across parties or ideologies. In contrast, maliciously engineered software—of the kind to which BMDs and other computerized components of a voting system are susceptible—is capable of systematically pushing an election results toward or away from a given candidate, party, or ideology.

17. Furthermore, modern optical scanners can be programmed to detect the most common types of errors by voters, such as overvotes and undervotes. Where ballots are scanned in-precinct, and the scanners are programmed correctly, the voter then has the opportunity to correct their ballot once the scanner reports the error. The Dominion optical scanners that the State intends to deploy offer this capability.

Dominion Voting Equipment has Serious Deficiencies

18. I have reviewed the Test Report issued by Pro V & V, Inc. containing the results of their functionality certification testing of the Dominion Voting Systems

D-Suite 5.5-A Voting System,⁵ referred to elsewhere in this Declaration as the Proposed Election System. I have also reviewed similar reports issued by five examiners appointed to conduct testing of the Dominion Voting System on behalf of the State of Texas (“Texas Reports”).⁶

19. All five Texas examiners highlighted deficiencies with the Dominion system, including issues affecting its reliability, accessibility, and security. These problems led Texas to deny certification of the Dominion system in June 2019.⁷

20. Several of the serious deficiencies noted by the Texas voting system examiners affect system components slated for use in Georgia, including:

- (a) “Multiple paper jams occurred on the ICP [optical scanner] during the examination. [...] This happened two times with only 60 ballots processed.”⁸

⁵ “Test Report, Dominion Voting Systems D-Suite 5.5-A Voting System Georgia State Certification Testing” (August 7, 2019) *available at* https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf (last visited Oct. 2, 2019).

⁶ “Examiner Reports of Dominion Voting System Democracy Suite 5.5” (Jan. 16-17, 2019) *available at* https://www.sos.state.tx.us/elections/laws/jan2019_dominion.shtml (last visited Oct. 2, 2019).

⁷ “Report of Review of Dominion Voting Systems Democracy Suite 5.5” (June 20, 2019) *available at* <https://www.sos.state.tx.us/elections/forms/sysexam/dominion-democracy-suite-5.5.pdf> (last visited Oct. 2, 2019).

⁸ Report of Texas examiner Tom Watson.

- (b) “Due to the frequency of paper jams, the ICP does not sufficiently preserve the secrecy of the ballot. The mechanism required to clear the paper jams does not keep the system safe from fraud or unauthorized manipulation.”⁹
- (c) “Another major concern is the quality of the scanned ballot images. Write-in selections written in ballpoint pen were illegible. Even the scanned images of ballots generated by Dominion’s own ballot marking devices were of poor quality.”¹⁰
- (d) “[H]aving the printer tray ajar during the voting process caused the system, after all the races are voted, to wipe out all selections and require the voter to start over after the print tray is fixed.”¹¹
- (e) “The ICXs [BMDs] are built with a [commercial off-the-shelf] tablet and printer. The Android OS versions used on the tablets are several years old, therefore they do not have the latest security feature [*sic.*] as later Android releases.”¹²

⁹ Report of Texas examiner Brandon Hurley.

¹⁰ Report of Texas examiner Brian Mechler.

¹¹ Report of Texas examiner Brandon Hurley.

¹² Report of Texas examiner Tom Watson.

(f) “The doors covering data and power ports on the [BMD] tablets do not provide sufficient protection. [...] a bad actor could add a USB device to the tablet while powered down that could remain undetected until after the election had ended.”¹³

(g) “The ICX [BMD] also presented problems during the accessibility testing portion of the exam which demonstrate that it may not be suitable as an accessible voting system.”¹⁴

21. The Pro V & V Test Report revealed an additional dysfunction: the ICP scanner lacks a memory-management unit (“MMU”). The immediate effect of the absence of an MMU was that the ICP needed rebooting after scanning approximately 4,000 ballots. More broadly, the absence of an MMU in the ICP scanner suggests that the scanner is based on hardware and software that is significantly out of date and out of step with current computer engineering practice.

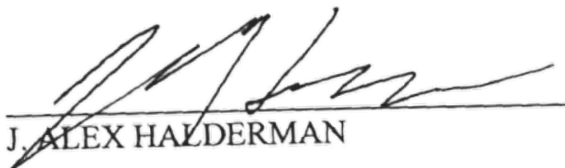
22. Likewise, Dominion’s response to the State’s request for proposals stated that the latest federally certified version of the Image Cast X BMD software

¹³ Report of Texas examiner Brian Mechler.

¹⁴ Report of Texas examiner Chuck Pinney.

used the Android 5.1 operating system.¹⁵ This fifth major version of Android is more than four years old and has not received security updates since March 2018. The *tenth* major version of Android became available in 2019. This is unfortunately consistent with the GEMS/DRE system, which relies on software so out of date that the manufacturer stopped providing updates and patches more than a decade ago.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 2nd day of October, 2019 in Bregenz, Austria.



J. ALEX HALDERMAN

¹⁵ Certificate of Conformance, Dominion Voting Systems Democracy Suite 5.5-A (Jan. 30, 2019) at pp. 3-4, *available at* <https://www.eac.gov/file.aspx?A=TQycVTA%2BOLpxoCbwCFjQJmJdRP1dq9sFO3oVUWJl5u4%3D> (last visited Oct. 2, 2019).