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.

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

DECLARATION OF J. ALEX HALDERMAN

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

1. The Court's recent Order (Doc. 579) "requires the State Defendants to develop procedures and take other actions to address the significant deficiencies in the voter registration database and the implementation of the ExpressPoll system." Specifically, it directs State Defendants to perform actions including:

(a) "to develop a plan, for implementation no later than January 3, 2020, that addresses the procedures to be undertaken by election officials to address errors and discrepancies in the voter registration database that may cause eligible voters to (i) not appear as eligible voters in the electronic poll books, (ii) receive the wrong ballot, (iii) be assigned to the wrong precinct

in the electronic poll book, or (iv) be prevented from casting a regular ballot in their properly assigned precinct"; and

(b) to work with cybersecurity consultants "to conduct an in-depth review and formal assessment of the issues related to exposure and accuracy of the voter registration database", including issues that apply to the new electronic poll book system.

2. While the Order does not specify a deadline for completing the review and formal assessment, an understanding of the deficiencies and likely failure modes of the current system is a necessary prerequisite for developing effective mitigations. Logic dictates that State Defendants must undertake the review before finalizing a plan to address the problems.

3. A wide range of technical issues could result in database "errors and discrepancies" that harm voters. For example, the electronic poll books themselves are a critical component of the database system. An attack that infected the poll books and erased their copies of the registration database during polling would cause lengthy delays and drive away many eligible voters. Even if a small number of paper printouts of the registration list were available, check-ins would be slowed dramatically, resulting in long lines. Similarly, issues that expose the content of the voter database to unauthorized parties could allow those parties to impersonate

voters and change their registration information, causing those voters to receive the wrong ballot or be prevented from casting a regular ballot.

4. An "in-depth review" of the voter registration issues raised in this matter would need to encompass all of the interconnected components that comprise the registration system, including: (i) the ElectioNet ("eNet") system used by election officials; the Georgia Online Voter Registration ("OVR") and My Voter Page ("MVP") websites used by the public; (iii) the current ExpressPoll poll books; (iv) the new Poll Pad poll books; and (v) the voter registration data itself. Attacks or data corruption affecting any of these components could threaten voters' ability to exercise their right to vote.

ElectioNet

5. ElectioNet ("eNet") is a voter registration data management application that election officials use to maintain the voter registration data and to export it to poll books for each election. In February 2018, Fortalice conducted a vendor cyber risk assessment of eNet that encompassed a contract and documentation review, network scans and reviews of server configurations, and interviews with key personnel at PCC, the vendor that developed and operates eNet. The assessment was limited in scope and did not include source code review or penetration testing. Even this limited review identified an array of serious security deficiencies in both the software and PCC's network environment. In July 2019, the SOS assumed

operational responsibility for eNet, but development and maintenance of the software continue to be the responsibility of PCC.[1]

6. Georgia plans to continue using eNet as part of the state's new voting system. The ExpressPolls will be replaced with Poll Pad poll books, and eligible voter lists will be exported from eNet to the Poll Pad system for each election. Therefore, securing eNet will remain critical for assuring the correct functioning of voter registration in future elections.

7. Merely transferring eNet operations to the SOS cannot mitigate the full range of issues identified by Fortalice, and there is no evidence that State Defendants have taken other steps to address them. Moreover, the 2018 security assessment was of limited scope, and a more thorough assessment, including a source code review and penetration tests, would be necessary to ensure that all relevant issues are discovered and corrected. The results of such an assessment are likely to have significant bearing on the design of appropriate mitigations for the voter registration system. For instance, a code review might show that fully mitigating the problems with eNet will require replacing or rewriting the software.

My Voter Page and Online Over Registration

8. An in-depth review of voter registration system security issues would also need to encompass the Georgia My Voter Page (MVP) and Online Voter

[1] Testimony of Merritt Beaver (Tr. Vol. 1, Doc. 570)

Registration (OVR) websites. These websites interface with eNet and use software developed by PCC to allow voters to view and update their voter registration data.

9. Serious vulnerabilities in the MVP website were discovered on the eve of the November 2018 election and reported to the SOS by Plaintiffs' counsel. Unauthorized parties could have exploited these vulnerabilities to access sensitive system configuration files and voter registration data. This information would have allowed attackers to fraudulently change voters' registrations through the OVR system. The SOS commissioned Fortalice to investigate whether the vulnerability had been maliciously exploited,[2] but no evidence has been presented about the outcome of that investigation.

10. Even cursory security testing should have uncovered the MVP vulnerabilities, and their existence calls into question the overall security posture of the MVP and OVR websites.[3] As with the eNet system, an in-depth review of the MVP and OVR systems would entail source code review, penetration testing, and follow-up to ensure that any discovered vulnerabilities are properly mitigated.

ExpressPoll Poll Books

11. The Court has specifically directed State Defendants to address the deficiencies in the implementation of the ExpressPoll system. While the

---

[2] C.A. No. 1:18-cv-5102-AT (N.D. Ga. 2018) (Doc. 39).
[3] The Court itself discovered what appears to be a security-related misconfiguration in the MVP website in August 2019 (Doc. 579 footnote 59).

ExpressPolls are slated to be replaced as part of Georgia's new voting system, they may need to be used into 2020 if the replacement poll books are delayed, and so prudent contingency planning calls for an in-depth review of their security posture.

12. There is no evidence that Georgia has ever performed a security review of the ExpressPolls. However, they were examined by the Secretary of State of Ohio in a rigorous source-code review and security test commissioned in 2007.[4] The Ohio study found several serious vulnerabilities. Georgia failed to apply software updates to its DREs to remediate vulnerabilities documented in the same Ohio study, and its ExpressPolls may also still be vulnerable.

13. Among the problems discovered in the Ohio study is that the "ExpressPoll will install an unauthenticated bootloader and operating system" from its memory card without authentication, allowing an attacker to replace the poll book's software with malicious code. This vulnerability is nearly identical to the flaw in the AccuVote DREs that Defendants' expert Dr. Michael Shamos called "one of the most severe security flaws ever discovered in a voting system."[5]

14. An attacker could exploit this vulnerability by tampering with the data that workers copy to the ExpressPolls before each election to load the list of eligible

---

[4] Patrick McDaniel et al., *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* (2007), Sec. 14.6. Available at https://www.eac.gov/assets/1/28/EVEREST.pdf

[5] Shamos Dep. at 115.

voters. An attacker who infected ExpressPolls in this way could cause them to turn away specific voters or classes of voters, or make them fail entirely on election day.

15. ExpressPolls are known to contain other longstanding software defects. For instance, Fulton County Director for Registration and Elections Richard Barron testified that under specific conditions the ExpressPoll will display information for the wrong voter, potentially causing poll workers to send the voter to an incorrect precinct.[6] This defect apparently dates back to at least 2006.

16. The presence of these vulnerabilities and defects indicates that other, undiscovered problems likely exist in the ExpressPoll software, and an in-depth review should include source code analysis and rigorous testing to identify other problems that could impair accuracy and data integrity. Until ExpressPolls are eliminated in Georgia, addressing their deficiencies will require a thorough understanding of their flaws.

Poll Pad Poll Books

17. As part of the new voting system, Georgia has selected an electronic poll book called the Poll Pad, which is manufactured by KnowInk, LLC.[7]

18. The Poll Pad system consists of off-the-shelf Apple iPad devices that run a custom software application that communicates with an Internet-based

---

[6] PX 16, Fulton county Board of Registration and Elections' Responses to Coalition Plaintiffs' First Interrogatories, Doc. 565-16 at 4.

[7] https://knowink.com/product-catalog/poll-pad/

administration system called ePulse.[8] Election workers use the ePulse website to upload lists of eligible voters for each precinct, manage Poll Pad devices, and retrieve voter history data after an election. Rather than using memory cards, the Poll Pads connect to the ePulse server over the Internet to retrieve the registration data.

19. When polls are open, Poll Pads can be configured in a fully connected mode, in which they continuously communicate with ePulse over the Internet, or in a peer-to-peer communication mode, in which they exchange data with other Poll Pads in the polling place over a Bluetooth or WiFi wireless network.

20. The Poll Pad is more complex than the ExpressPoll system, due to its Internet connectivity and multiple modes of wireless data transfer, but the Georgia SOS approved its use without conducting any security testing. In fact, Georgia certified the new voting system without performing security testing or source code review of any of the components. The certification was preceded by tests performed by Pro V&V, which were limited to checking functional compliance with Georgia requirements.[9] The test report states that testing "was not intended to result in exhaustive tests of system hardware and software attributes; these are evaluated during federal compliance testing." However, Federal voting system guidelines do

---

[8] The functionality of the Poll Pad system is described in detailed manuals posted by California:
https://votingsystems.cdn.sos.ca.gov/vendors/knowink/mastermanual.pdf
https://votingsystems.cdn.sos.ca.gov/vendors/knowink/ki-user-guide.pdf

[9] https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf

not cover poll books, and so the Poll Pad has not been federally tested or certified. The word "security" does not appear in the Pro V&V report.

21. In contrast, the Secretary of State of California conducted a source code review[10] and penetration testing[11] of the Poll Pad in 2018. Among several significant deficiencies found by California were: (i) cross-site scripting vulnerabilities and insecure use of HTTP Cookies in the ePulse website, which could allow attackers to hijack election officials' accounts; (ii) the ability of the software to delete log files without this action itself being logged, which could help attackers hide evidence of their activities; and (iii) improper programming structures that apparently created the potential for inadvertent data loss.

22. Following these tests, California conditionally certified the Poll Pad subject to 19 terms and limitations that reflect the findings of the security testing.[12] Among the conditions is that Poll Pads may not be connected to smart card encoders, so that there is no path for an attack to spread from the poll books to voting machines.

23. Pennsylvania also evaluated and conditionally certified the Poll Pad in 2018.[13] The Pennsylvania certification is subject to 24 conditions and accompanied by five additional security recommendations. The conditions include that Poll Pads

---

[10] https://votingsystems.cdn.sos.ca.gov/vendors/knowink/source-code-report.pdf
[11] https://votingsystems.cdn.sos.ca.gov/vendors/knowink/security-report.pdf
[12] https://votingsystems.cdn.sos.ca.gov/vendors/knowink/cert.pdf
[13] https://www.dos.pa.gov/VotingElections/Documents/Voting Systems/Knowink PollPag 1.3.3/Knowink Poll Pad 1.3.3 Approval Report.pdf

must not be configured to communicate with ePulse over the Internet during polling, and that Poll Pads and their removable media must never be connected to other voting system components, including a prohibition of using the Poll Pads to encode voter access cards.

24. It is unclear what conditions, if any, Georgia plans to impose on use of Poll Pads. However, Pro V&V's functional tests included testing that the Poll Pad was able to encode voter activation cards for use with the new Dominion BMDs. California and Pennsylvania prohibit use of this function, as it could create a way for an attack to spread from the Poll Pads to the rest of the voting system.

25. As part of an in-depth registration security assessment, Georgia should commission source code review and penetration testing of the Poll Pads and their Internet-based components. As in California and Pennsylvania, procedural mitigations should be developed based on the results of such testing.

Voter Registration Data

26. The longstanding security issues with eNet and other registration system components raise the possibility that data housed in the voter registration database is *already* inaccurate, due to past attacks or software errors.

27. State Defendants assert that registration data transferred to the new voting system must be "scanned 'with anti-malware software' before it can be imported" (Doc. 556). Commercial anti-malware scanning is unlikely to detect

attempts by nation-state attackers to spread targeted malware. Moreover, anti-malware software cannot stop errors from propagating if the registration data is corrupted before being transferred.

28. Assessing the integrity and accuracy of existing registration data is important no matter what other security improvements the state implements going forward. Such an assessment should include comparing current voter registration data to backups from previous election cycles and auditing the records that have changed. Georgia's recent participation in the multistate Electronic Registration Information Center (ERIC) may also be an important part of a data validation plan

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 26th day of August, 2019 in Rushland, Pennsylvania.

J. ALEX HALDERMAN