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

Pursuant to 28 U.S.C. § 1746, I, J. ALEX HALDERMAN, declare 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. In August 2020, the Court granted Plaintiffs access to Georgia voting equipment for the purpose of assessing its security. I examined the equipment for the Curling Plaintiffs, with the assistance of Professor Drew Springall of Auburn University. In just twelve person-weeks of work, we discovered numerous vulnerabilities, some of which could potentially be exploited to alter election results.

I submitted an Expert Report dated July 1, 2021, that describes these vulnerabilities and explains the threats they pose to future elections in Georgia.

3. In December 2021, the Court ordered the parties to convey the Expert Report to Dominion so that the company could begin patching the vulnerabilities to the extent possible. In February 2022, the Court further ordered Curling Plaintiffs to submit the Expert Report to CISA's Coordinated Vulnerability Disclosure (CVD) program so that the agency could advise affected jurisdictions about the problems. CISA published a Security Advisory summarizing some of the vulnerabilities in June 2022. Dominion subsequently developed an updated version of its software, Democracy Suite 5.17, that is intended to address some of the vulnerabilities in the Expert Report as well as the DVSorder privacy vulnerability that I discovered independently of this lawsuit.[1] The updated Dominion software received EAC certification in March 2023.

4. Plaintiffs, State Defendants, CISA, Dominion, numerous cybersecurity experts, and I all agree that the Court should unseal the Expert Report and allow it to be made public, subject only to certain narrow technical redactions. However, the

[1] I cannot say whether Dominion's new software successfully address any of these issues, because I have not been given access to the new software to validate the changes (nor, to my knowledge, has CISA been given such access).

Court, quite understandably, has asked whether releasing the Expert Report would "compound the threats and risks to the security of the voting system". Making vulnerability information public is never without risk; however, in this instance, keeping the Expert Report secret would carry far greater risks than making it public.

5. Maintaining the Expert Report under seal (other than the previously proposed redactions) would do little or nothing to hinder serious adversaries. Indeed, part of the reason that the vulnerabilities in the Dominion system are so dangerous is that they are easy to discover given access to the software, which is now widely available. Professor Springall and I found them without expending extensive resources or unusual expertise, but rather merely by applying widely held knowledge about computers and security over a span of a few weeks. Georgia's Dominion software fell into the hands of unauthorized parties more than two years ago in the Coffee County breach, and it has been widely disseminated. Similar Dominion software was stolen from Mesa, Colorado in 2021 and can be downloaded by anyone online. Regardless of whether the Expert Report is made public, adversaries can study the leaked software to discover the same or equivalent vulnerabilities. In my assessment, access to the Expert Report would save such adversaries *at most* a few weeks of effort, and probably less, since CISA's public Security Advisory already

contains numerous clues about where in the software the vulnerabilities are to be found.

6. Furthermore, while the Expert Report may appear to give a "roadmap" for attacking the election system, it stops well short of providing complete recipes for exploiting the most dangerous attacks. For instance, the Expert Report omits numerous technical details about the vote-stealing malware it describes, since these details are not needed for the Expert Report's analysis and conclusions. Anyone seeking to create real malware would need to figure out these details on their own, since the source code for the malware that Professor Springall and I developed will remain secret under this Court's Protective Order even if the Expert Report is unsealed. The redactions I previously proposed would withhold other key technical details that attackers would need. Adversaries who are technically proficient enough to work out these details if the Expert Report is made public would be equally capable of discovering the complete vulnerabilities without access to the report.

7. Any risk to making the Expert Report public needs to be balanced against the benefits to election security and transparency that unsealing it would provide. Access to the Expert Report will give election officials and other policymakers a more complete picture of the Dominion equipment's security risks, which will help them make better-informed decisions about how to defend it. For

instance, several states are now performing testing and certification for Dominion's updated software, but without access to the Expert Report, they do not have enough information to test whether Dominion's changes properly mitigate some of the vulnerabilities. Access to the Expert Report is also crucial for helping states assess the magnitude of the risks that the vulnerabilities create, since although CISA's Advisory states that the problems "should be mitigated as soon as possible", it does not provide specific information regarding the ease with which they can be discovered and exploited.

8. Withholding the Expert Report also hinders states' efforts to mitigate the vulnerabilities and corresponding threats to elections. CISA has urged states to adopt a long list of mitigations, which run the gamut from tweaking specific technical settings ("Disable the 'Unify Tabulator Security Keys' feature") to implementing broad policies ("for each election […] Conduct rigorous post-election tabulation audits"). Yet without the details from the Expert Report, officials cannot understand why each mitigation is necessary, let alone determine what the consequences will be if some mitigations are not implemented or are imperfectly applied. Unsealing the Expert Report will allow states' security experts to understand the vulnerabilities in sufficient depth to make appropriate recommendations on such matters and for the

states themselves to understand the specific steps needed to mitigate those vulnerabilities, to the extent possible.

9. Beyond helping to secure elections that rely on Dominion's equipment, unsealing the Expert Report will inform broader policy discussions that are taking place now in state legislatures and in Congress. For instance, Louisiana will soon decide whether to purchase a BMD-based voting system like Georgia's or a predominantly hand-marked system—a choice for which the risks discussed in the Expert Report are extremely relevant. (Louisiana previously requested permission from the Court to access the Expert Report, and that request was denied.) In the U.S. Senate, lawmakers are considering a bill to require the EAC to perform penetration testing as part of its certification process—a reform for which the Expert Report would provide important information and context, since it is essentially a compendium of serious failings with Dominion's voting equipment overlooked by the existing EAC certification process.

10. Meanwhile, in Georgia, the Secretary of State's Office has done little, if anything, to implement the mitigations prescribed by CISA, and recently made the stunning admission that it may not get around to installing Dominion's security patches until after the 2024 Presidential Election.

11. One reason for this lack of urgency may be the fact that Dominion has told Georgia (and other jurisdictions that use Dominion's voting equipment) that MITRE concluded the attacks in the Expert Report are infeasible. This is highly misleading. MITRE admits it was provided no access to Dominion's equipment or software (unlike Professor Springall and myself), and MITRE's analysis is entirely premised on the false assumption that outsiders cannot gain access to the equipment and software—which outsiders *did* in Coffee County and elsewhere. Security experts who advise states cannot properly assess MITRE's claims and understand why they are unfounded and dangerous without the same access to the Expert Report that MITRE received from Dominion.

12. For these reasons, the balance of security interests heavily favors unsealing the Expert Report now, while Georgia and other states still have almost 18 months to address the vulnerabilities ahead of the next presidential election.

13. Unsealing the Expert Report now will also defuse the risk that it could become public without authorization. Through no fault of Plaintiffs or their experts, a large number of people and organizations have come to possess copies of the

Expert Report,[2] creating a substantial risk that it will be accidentally disclosed, stolen, or even deliberately leaked. I am especially fearful that the Expert Report will be leaked around the time of the 2024 Presidential Election to cause chaos or undermine the legitimacy of whoever wins in Georgia. This is even more likely if Georgia fails to patch the vulnerabilities by that time, as it appears set to do.

14. There is ample time for states to adopt wider use of hand-marked paper ballots, implement rigorous post-election audits, install software patches, and implement other defenses to improve their security posture in response to the vulnerabilities the Expert Report describes. That will not be true a year from now, and it becomes increasingly difficult the longer the Expert Report remains unavailable to those who need it to understand the specific risks the Dominion's voting equipment and software present and the specific measures needed to mitigate those risks.

---

[2] The Court authorized the Report's dissemination to counsel and experts for the parties in this lawsuit, Georgia state officials, Dominion, and CISA, which shared it with EAC and DOJ as part of the CVD process. Dominion shared it without the Court's authorization with MITRE as well as with counsel and experts for the parties in the company's recently settled defamation suit against Fox News. Dominion has similar lawsuits pending against Mike Lindell and My Pillow; against Newsmax, One America News, and Patrick Byrne; against Rudy Giuliani; and against Sidney Powell and related parties. I understand that Dominion has declined to disclose whether it produced the Expert Report to those parties, their counsel or experts, or others, despite requests from Plaintiffs here for such clarity.

15. Unsealing the redacted Expert Report now, when it may help spur critical mitigations, is needed to advance the public's interest in secure elections. Unfortunately, for the reasons I explain in the Expert Report and in other testimony I have provided in this matter, releasing the Expert Report will not provide the level of security required to reasonably protect elections against interference and failures arising from use of Dominion's unreliable voting equipment in the current climate. The many serious failings with that equipment, as confirmed by CISA, present numerous opportunities for bad actors (including what State Defendants and Dr. Michael Shamos call "insiders") to adversely affect individual votes and even election outcomes, especially in the current environment of advanced persistent threats to U.S. elections, as acknowledged by federal authorities. This is especially true given the ease with which potentially bad actors can breach the Dominion voting system and gain unfettered access to it in its operational environment—as occurred in Coffee County—after having had access to the Dominion software for years to identify its many serious vulnerabilities and devise ways to exploit them. Continuing to seal the redacted Expert Report will only exacerbate those very serious security failings, whereas releasing it will provide at least some help to mitigate them—including by providing vital information that election officials need to make

informed decisions about whether to purchase the equipment or whether to continue using it, and if so, exactly how.

16. Releasing the redacted Expert Report also will provide critical information for voters to understand the risks the vulnerable equipment poses to their right to vote, enabling them to make informed decisions about whether to vote on the BMDs and whether to support elected officials who adopted and are maintaining the vulnerable equipment (especially without implementing the requisite mitigation measures), as in Georgia. In sum, while releasing the redacted Expert Report will not remedy the inadequacy of the Dominion BMD system that renders it inappropriate for U.S. elections, it will help stakeholders—including both election officials and voters—make informed decisions and take necessary steps to mitigate the threats that system poses to elections.

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 16th day of May, 2023 at Ann Arbor, Michigan.

J. ALEX HALDERMAN