**Elections Commission**
***City & County of San Francisco***
Lucy Bernholz, President
Charles Jung, Vice President
Christopher Jerdonek
Becca Chappell
Viva Mogi

John Arntz, Director of Elections
Martha Delgadillo, Secretary

Secretary of State Shirley N. Weber, PhD.
1500 11th Street
Sacramento, CA 95814

Via email

January 28, 2022

Dear Secretary of State Weber:

I am writing in my role as President of the San Francisco Elections Commission ("Elections Commission") in response to material brought to our attention regarding the security of Dominion Voting Systems equipment. The information comes from a legal suit filed in the State of Georgia alleging security issues with elements of Dominion Voting Systems. As part of that case, an independent security expert was hired to audit the system. It is the findings of that audit that raise concerns.

Attached to this letter please find materials submitted to, and reviewed by, the Elections Commission. These materials, which were submitted to the Elections Commission by Dr. David Jefferson, a retired computer science faculty member from UCLA, include:

- Cover letter from Dr. Jefferson
- Declarations from the independent auditor, J. Alex Halderman
- Motions to the GA Court by the Louisiana Secretary of State
- GA Court order in response to Louisiana Secretary of State
- Memorandum to the GA Court in Support of LA SoS Motion from Fox News

As we are only one of the many counties in California that use Dominion Voting Systems equipment (see this list of Voting Technology By County, produced by your office https://votingsystems.cdn.sos.ca.gov/oversight/county-vsys/vot-tech-by-counties-2021-2.pdf) and because equipment certification is your office's responsibility, we believe these concerns are most appropriately addressed by the Secretary of State, not at the local jurisdictional level.

On behalf of the voters of San Francisco and the State of California, we urge you to investigate these matters and consider filing for a Limited Motion to Intervene to gain access to the findings of the security audit and to take such actions as your office deems necessary to ensure the security of these systems, which are already in use across the State. We also request acknowledgment of this letter and the release to the public of such materials as possible.

.

Thank you for your attention and your timely response to this inquiry.

Sincerely,

Lucy Bernholz
President, San Francisco Elections Commission

cc: Members of the San Francisco Elections Commission
San Francisco Director of Elections John Arntz
Deputy City Attorneys Andrew Shen and Ana Flores
Dr. David Jefferson, retired faculty, UCLA

January 2, 2022

Dear Members of the San Francisco Elections Commission,

I am writing to let you know about a recent report of security vulnerabilities in Dominion's ImageCast X voting system and to encourage you to obtain a copy of that report. The vulnerabilities are potentially very serious. I understand that San Francisco uses the Dominion ImageCast X, primarily for voters with disabilities, and thus, I think it is important for you to obtain this information so you can know whether and how you may be affected.

I hasten to add that my alerting you to these issues with the ImageCast X equipment has nothing to do with the widespread conspiracy theories circulating in the right-wing press about Dominion voting systems, and I am not suggesting that there is any evidence of actual fraud or error in any past elections traceable to the Dominion machines.

Let me also note that I am a computer scientist, a former professor at UCLA, and now retired from Lawrence Livermore National Laboratory. I have been studying, writing, and testifying about voting system security for well over 20 years, serving as an advisor of one kind or another on election security matters to six Secretaries and Acting Secretaries of State of California. I am also a long-time former Board member of both Verified Voting and the California Voter Foundation. I have been a nonpartisan activist for election security in many states and at the federal level for all that time.

The state of Georgia uses the same Dominion machines for all its voters that San Francisco uses for voters with disabilities. You may be aware that there is a long-running federal court case in the Northern District of Georgia, Curling v. Raffensperger, in which the plaintiffs argue that these machines should be declared removed from service. Many distinguished voting system experts have testified or submitted declarations to the Court on the side of the plaintiffs, including University of Michigan Prof. Alex Halderman, U.C. Berkeley Prof. Philip Stark, famed security expert and white hat hacker Harri Hursti, Princeton Prof. Andrew Appel, and Georgia Tech Prof. Rich DeMillo.

I am attaching two of Prof. Halderman’s public declarations (redacted under the rules of the Court), but I want to call your attention especially to a third declaration of his that is currently sealed by the Court. The Court allowed Prof. Halderman to examine and test the ImageCast X machines used in Georgia, and he found profoundly dangerous security flaws and vulnerabilities in them. He submitted it as sealed under Court rules. Apparently the concerns he expressed in his report are so serious that the Court is concerned that making it public might aid potential attackers and perhaps undermine the confidence of the electorate in Georgia elections.

Only a handful of people have been allowed to read Halderman’s sealed report to the Court, and I am not among them. However, having led prior studies of voting system vulnerabilities I am familiar with the *kinds* of flaws that Halderman may have found in the ImageCast X, and they are extraordinarily serious. In a prior public declaration that is heavily redacted, Halderman wrote that the ImageCast X machines are “even easier to compromise then the DRE equipment it replaced". (See attachment, dated 2021-02-12, p. 9). The prior DRE machines used in Georgia were the notorious Diebold AccuVote TS systems, famous for being exploitable with access only to a removable memory card. Through that card it is possible, among other things, to inject a malicious virus that can spread to all the machines in a jurisdiction, including the central server. In the first stage of the Curling litigation the Court declared those Diebold DREs to be unconstitutional.

I believe it is important for San Francisco election officials to obtain a copy of Halderman's sealed report and evaluate it for yourselves in the context of elections here. Recently, in November 2021, the Court has indicated it will consider access to the report for officials with a *bona fide* need for it, provided they offer assurances that they will protect the report from being made public and will limit its circulation to the minimal number of people needed for proper evaluation. Officials in the State of Louisiana have already submitted such a motion (attached), and the Court has yet to rule on it. I suggest that you might model your request on their motion. Alternatively, you might ask for a redacted version of Halderman's report, which might be easier to get and require fewer restrictions.

I really hope that you will take the initiative to see for yourselves what the vulnerabilities are in the ImageCast X that Prof. Halderman is warning about in such strong terms. I have a little more information about this and would be glad to answer any questions you have (or get the answers) at a future meeting or otherwise if that would be helpful. Feel free to contact me at any time.

Sincerely,
David R. Jefferson
David R. Jefferson
drjefferson@gmail.com
925-989-3701

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

| | |
|---|---|
| **DONNA CURLING, ET AL.,**<br>**Plaintiffs,** | |
| **v.** | **DECLARATION OF**<br>**J. ALEX HALDERMAN** |
| **BRAD RAFFENSPERGER, ET AL.,**<br>**Defendants.** | **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. At a general level, my analysis of Georgia's new election equipment has revealed that, despite the addition of a paper trail, individual Georgia voters who use BMDs face security risks that are *worse* than the risks they faced when voting on DREs.

3. Paper ballots and risk-limiting audits are often thought of as the "gold standard" for election security, because, when applied in certain ways, they can detect

and correct any outcome-changing cyberattack on the election technology. Yet, in Georgia, a series of missteps in the design and implementation of the election system have rendered these critical protections ineffective. These missteps and other security defects expose Georgia voters to severe risks that their individual votes will not be counted accurately, if at all.

4. Georgia requires nearly all in-person voters to use BMDs. These voters' ballots are counted based on barcodes, which voters cannot read or verify. While the ballots also contain human-readable text, with rare exceptions this text is completely ignored during counting. (State rules call for using a risk-limiting audit to confirm that the election outcome matches the human-readable portion of the ballots in only a single contest every two years, and even in the event of a candidate-initiated recount, the election result is typically determined from the barcodes.) As a result, an attacker who could infiltrate the BMDs and manipulate the barcodes could change votes for individual voters such as Curling Plaintiffs without detection, as if the paper trail did not exist. This could be done in a manner that does or does not affect the election outcome, depending on the manner of the attack—but the result nonetheless would be the alteration or loss of personal votes for the individual voters affected.

5. The risk of such an attack depends on the feasibility of hacking an individual BMD to manipulate votes without detection, such as by altering the

corresponding barcodes. Where the objective of the attack also is to alter an election outcome, the risk additionally would depend on the likelihood that attackers can compromise *sufficiently many* votes (across multiple BMDs, depending on the election) to accomplish that objective. The Plaintiffs have asked me to perform technical assessments of these risks.

6. [redacted]

7. [redacted]

[1] Halderman Decl. (Dec. 16, 2019), Dkt. 682 at ¶ 8.

[redacted].[2]

8. [redacted]

[redacted]

[redacted]

[redacted]

9. [redacted]

[2] [redacted] Dckt. 906 at 31:12-18.

[redacted]

10. [redacted]

[3] *See*: Secretary of State's Office, "Secretary Raffensperger announces completion of voting machine audit using forensic techniques: No sign of foul play," (Nov. 17, 2020), available at https://sos.ga.gov/index.php/elections/secretary_raffensperger_announces_completion_of_voting_machine_audit_using_forensic_techniques_no_sign_of_foul_play.

[redacted]

11. [redacted]

12. Beyond demonstrating the feasibility of altering personal votes cast by individual voters on individual BMDs, the Curling Plaintiffs seek to prove that such an attack could be accomplished on a wide scale, depriving them and other Georgia

voters of their right to vote. There is a growing body of evidence that this is the case, beginning with Georgia's record of major election security lapses, such as the vulnerabilities at the Center for Election Systems discovered and exploited by Logan Lamb, the vulnerabilities in the online voter registration system that came to light on the eve of the 2018 general election, and the problems identified by Fortalice in the Secretary of State's computing infrastructure. Additional discovery is necessary to assess the full extent to which similar security gaps can facilitate wide-scale attacks on the BMDs.

13. [redacted]

14. [redacted]

15. [redacted]

[4] Dkt. 892-11.

16. The Curling Plaintiffs' technical investigations, as I understand the scope of my assignment in this case, are not intended to show that the outcome of any past election was maliciously altered. I understand that my assignment is not to analyze any specific election outcomes because the Curling Plaintiffs brought this case to protect their personal and individual right to vote, regardless of the outcome of any election, past or future. What my analyses demonstrate is that Curling Plaintiffs cannot be assured that the personal votes each of them casts on BMDs as individual voters will be counted correctly or perhaps at all. I expect that the further analyses I plan to conduct in this case, including with additional discovery, will further confirm this fact.

17. Unfortunately, the analysis I have conducted already shows that Georgia's new BMD equipment is even easier to compromise than the DRE equipment it replaced.

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 12th day of February, 2021 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

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

| | |
|---|---|
| **DONNA CURLING, ET AL.,**<br>**Plaintiffs,** | |
| **v.** | **DECLARATION OF**<br>**J. ALEX HALDERMAN** |
| **BRAD RAFFENSPERGER, ET AL.,**<br>**Defendants.** | **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. I have reviewed the expert disclosures prepared by Dr. Juan Gilbert and Dr. Benjamin Adida for State Defendants. Neither Dr. Gilbert not Dr. Adida offers any rebuttal to the numerous, critical vulnerabilities in Georgia's BMDs that I described in my July 1, 2021 expert report. Dr. Adida did not respond to my report at all; State Defendants reissued prior declarations from him previously provided in this litigation. Neither of them disputes the presence of any of the serious

vulnerabilities I detail in my report or the steps I describe for exploiting those vulnerabilities to alter individual votes and election outcomes in Georgia. Nor does either of them claim to have examined any of the voting equipment used in Georgia to evaluate whether the vulnerabilities I identified—or others—have been exploited in any past election. Although each of them presumably could do this with the permission of State Defendants, who I understand engaged them as experts in this case, there is no indication either has undertaken any such inquiry or asked to do so. As a result, neither Dr. Gilbert nor Dr. Adida has anything to say about the reliability of the voting equipment used in Georgia elections. This is surprising, given that they have had at least the last year to examine Georgia's voting equipment.

3. State Defendants urgently need to engage with the findings in my report and address the vulnerabilities it describes before attackers exploit them. Nothing in Dr. Gilbert's or Dr. Adida's responses indicates that State Defendants understand the seriousness of these problems or have taken any measures to address them and their implications for the Plaintiffs' individual votes in future elections. Established practice in the security field would require State Defendants to promptly subject Georgia's voting system to rigorous testing in response to my report, to assess the extent and significance of each of the vulnerabilities I described, and to identify and *promptly implement* specific measures (where possible) to eliminate or mitigate each

of those vulnerabilities. Neither Dr. Gilbert nor Dr. Adida indicates any such efforts on their own part or on the part of State Defendants or anyone else. Again, Dr. Adida did not respond to my report.

4. In my report—a 25,000-word document that is the product of twelve weeks of intensive testing of the Dominion equipment provided by Fulton County—I find that Georgia's BMDs contains multiple severe security flaws. Attackers could exploit these flaws to install malicious software, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. I explain in detail how such malware, once installed, could alter voters' votes while subverting all the procedural protections practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs). Finally, I describe working proof-of-concept malware that I am prepared to demonstrate in court.

5. My report concludes, *inter alia*, that Georgia's BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors who are likely to target future elections in the state; that the BMDs' vulnerabilities compromise the auditability of Georgia's paper ballots; that the BMDs can be compromised to the same extent as or more easily than the DREs they replaced; and that using these vulnerable BMDs for all in-person voters, as Georgia

does, greatly magnifies the level of security risk compared to using hand-marked paper ballots and providing BMDs to voters who need or request them.

## **Reply to Declaration of Dr. Juan Gilbert**

6. Rather than engage with the facts in my report, Dr. Gilbert responds largely with vague generalities. He gives no indication that he has ever used an ICX BMD, let alone tested its security. He begins by conceding that "any computer can be hacked," but he contends that "this general statement is largely irrelevant," because hand-marked paper ballot systems use computers too (to scan the ballots) (¶ 6). His position is inconsistent with accepted standards for election security and with the facts of the particular voting system used in Georgia.

7. My testing has shown that the BMDs used in Georgia suffer from specific, highly exploitable vulnerabilities that allow attackers to change votes despite the State's purported defenses. There is no evidence that Georgia's ballot scanners suffer from the same extraordinary degree of exploitability, nor does Dr. Gilbert contend they do. He ignores the relative ease with which Georgia's BMDs can be hacked, including by a voter in a voting booth in mere minutes. That extreme difference in security as compared to other voting technologies, particularly hand-marked paper ballots, is far from "irrelevant" as Dr. Gilbert implies.

8. Furthermore, even if the scanners were just as insecure as the BMDs, Georgia's practice of requiring essentially all in-person voters to use highly vulnerable BMDs would needlessly give attackers *double* the opportunity to change the personal votes of individual Georgia voters, since malware could strike either the BMDs or the scanners. Accepted standards in election security compel reducing points of attack for bad actors, not unnecessarily expanding them—a point Dr. Gilbert ignores.

9. Lastly, Dr. Gilbert also ignores that accepted election security protocols include an effective measure to protect against hacks of ballot scanners when the ballots are hand-marked rather than generated by BMDs—namely, reliable risk-limiting audits (RLAs), which would have a high probability of detecting any outcome-changing attack on the scanners. Not only do Georgia's BMDs defeat the efficacy of RLAs, but Dr. Gilbert continues to ignore the fact that Georgia requires an RLA of just one statewide contest every two years (and, to my knowledge, has not adopted specific, adequate procedures to ensure a reliable RLA for that one audit every other year).

10. Dr. Gilbert goes on to discuss issues related to voter verification of BMD ballots (which I respond to below). Yet he fails to address the potential for attackers to cheat by changing only the QR codes printed by Georgia's BMDs.

Voters cannot read the QR codes, but they are the only part of the ballots that the scanners count. My report details several routes by which malicious hardware or software can manipulate the QR codes and cause the recorded votes to differ from voters' selections. In principle, a rigorous risk-limiting audit would be likely to detect such an attack if the attacker changed enough votes to alter the outcome of the contest being audited, but again Georgia rules require such an audit in only a single statewide contest once every two years. As my report explains, this leaves the vast majority of elections and contests in Georgia vulnerable to QR code (and others) attacks, yet Dr. Gilbert says nothing about this threat.

11. Instead, Dr. Gilbert focuses exclusively on a different threat: attacks that change *both* the QR codes and the ballot text. In addition to the barcode-only attacks I just discussed, my report demonstrates that Georgia's BMDs can be manipulated so that both the barcodes and the printed text indicate the same fraudulent selections. No audit or recount can catch such fraud, because all records of the voter's intent would be wrong. The only reliable way to detect it would be if enough voters carefully reviewed their ballots, noticed that one or more selections differed from their intent, and reported the problems to election officials, *and* if Georgia officials then discerned from the pattern of voter reports that the BMDs were systematically misbehaving. Thus, Dr. Gilbert is mistaken when he contends that the distinction

between "voter-verifiable" and "voter-verified" paper ballots "only matters in principle" (¶ 7). All BMD ballots are potentially voter-verifiable, but unless enough BMD ballots are actually voter-*verified*, BMD-based attacks could alter election outcomes even in the rare instances where the State conducts a risk-limiting audit. And unless *every* BMD ballot is actually voter-*verified*, BMD-based attacks could alter individual voters' selections without detection..

12. A large body of recent scientific evidence has established that few voters are likely to catch errors caused by malicious BMDs. I have reviewed this evidence in previous declarations.[1] It comes from both field observations (which report how long real voters review their ballots during real elections) and laboratory tests (which report the fraction of errors that subjects detect when voting on hacked BMDs in simulated elections). These methodologies are complementary, and results to-date from all studies of both kinds point to a low rate of voter-verification.

13. Dr. Gilbert criticizes field observations because "[t]ime spent reviewing a ballot has little to do with whether it was actually verified" (¶ 9). This claim is inconsistent with accepted election security principles. Of course, they are not exactly the same question, but obviously the time spent reviewing a ballot can

[1] *Halderman decl.* (Dec. 16, 2019), Dkt. 682 at 23-33; *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 6-8, 55.

provide important insight into whether it was likely verified. For example, we can conclude that a voter who spends only a second or two reviewing a lengthy, complicated ballot is unlikely to have reliably verified each of their selections on the ballot. And of course, the same is true for a voter who spends no time at all reviewing their ballot. Review time is both practical to measure and clearly correlated with the error detection success, making it a valuable and relevant metric, as multiple studies confirm.

14. Dr. Gilbert seems to contend, without evidence, that a casual glance is sufficient to review Georgia-style ballots because selections are printed together with party affiliations (¶ 9). He cites no research (and I am unaware of any) that supports this conclusion, particularly when, as in Georgia, the party affiliations are printed in small type and in a different horizontal position for each contest. A real BMD ballot is reproduced on page 15 of my expert report. This is just one example of such a ballot; they can be longer and more confusing. Dr. Gilbert provides no basis for believing that voters would likely catch deliberate errors caused by compromised BMDs when voting such a ballot.

15. Dr. Gilbert references my award-winning peer-reviewed study about voter verification behavior, which found very poor rates of error detection and

reporting in a mock election using BMDs that my team hacked (¶ 10).[2] He contends that my study "ignores the reaction to such manipulation in an actual election, particularly one as heated in the public domain as the 2020 Election." (¶ 11). He does not explain how or why such circumstances would be expected to materially increase voter verification of their respective BMD ballots, nor does he cite any support for his claim to believe they would. And, just last week, the Atlanta Journal-Constitution obtained a study (under the Georgia Open Records Act) commissioned by the Secretary of State's Office in which researchers from the University of Georgia observed Georgia voters during the November 2020 election and reported how long they spent reviewing their BMD ballots.[3] Although it appears the Secretary of State had this study at the time of Dr. Gilbert's response to my report, he does not address or acknowledge it. The new study suggests that voters in the real world review their ballots *even less carefully* than voters in recent laboratory studies—despite the reminders election workers are supposed to give them to carefully review

[2] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" In *41st IEEE Symposium on Security and Privacy* (May 2020). Available at https://ieeexplore.ieee.org/document/9152705.

[3] Mark Niesse, "Under half of Georgia voters checked their paper ballots, study shows," *Atlanta Journal-Constitution* (July 27, 2021). Available at https://www.ajc.com/politics/under-half-of-georgia-voters-checked-their-paper-ballots-study-shows/6HSVHHFOBRBDPODRZXLIBTUS64/.

their ballots at the polling sites, which Dr. Gilbert emphasizes as a remedy for poor voter verification of BMD ballots.[4]

16. The University of Georgia researchers report that 20% of voters they observed did not check their ballots at all.[5] Only about 49% examined their ballots for at least one second, and only 19% did so for more than five seconds. This is significantly worse performance than observed in my study, which found that when voters were verbally prompted to review their ballots before casting them, as should occur in Georgia, 63% of voters reviewed their ballots for only *two* seconds or more, compared to 19-49% in the new study.

17. This suggests that laboratory studies like mine tend to *overestimate* the rate at which real Georgia voters would detect errors on their BMD ballots. Since real Georgia voters were observed to review their ballots even less carefully than the

[4] Secretary Raffensperger appears to disagree with Dr. Gilbert about the value of measuring voter review time for assessing voter verification performance. He told the Atlanta Journal-Constitution that the new study "shows voters do indeed review their ballots for accuracy before casting them" and offers "proof the votes that were counted were for the candidates the voters intended." (*Id.*). I agree that the new study provides valuable insights about voter behavior, but, contrary to the Secretary's pronouncements, the results indicate that real Georgia voters are even less likely to detect errors caused by compromised BMDs than previous studies have suggested.

[5] Audrey A. Haynes and M.V. Hood III, "Georgia Voter Verification Study" (January 22, 2021). Available at https://s3.documentcloud.org/documents/21017815/gvvs-report-11.pdf.

participants in my study, it is reasonable to infer that real voters would catch an even smaller fraction of errors. The participants in my study who were similarly prompted to review their ballots caught 14% of errors. Therefore, real voters in Georgia are likely to catch substantially less than 14% of errors.

18. How often would voters have to detect errors on their BMD ballots to effectively safeguard against attacks? The answer depends on the margin of victory, since an outcome-changing attack would need to change fewer votes in a close contest. The model from my study shows that, given the margin of victory from the 2020 Presidential contest in Georgia, voters would need to have detected 46% of errors for there to be even one error report per 1000 voters, under a hypothetical scenario where the election outcome had been changed by hacked BMDs.[6] The University of Georgia observations show that barely 49% of voters looked at their ballots for even a second, let alone studied them carefully enough to reliably spot errors.

[6] To reiterate, the November presidential race was the only state-wide contest subjected to a risk-limiting audit. In other contests, attackers could change the outcome by tampering with only the ballot QR codes, and voters would have no practical way to detect this manipulation regardless of how diligently they reviewed their ballots.

19. Dr. Gilbert performs a similar calculation using the baseline error detection rate measured in my study. He finds that an outcome changing attack on Georgia's Presidential contest would have resulted in only 832 voters noticing that their BMD ballots showed the wrong selection. Dr. Gilbert suggests that there have not been such complaints from any voters, and says he finds it implausible that so many voters would have "simply not said anything or otherwise simply corrected their ballot and thought nothing of it then or since" (¶ 12).

20. This is an oddly constructed hypothetical, since Curling Plaintiffs do not claim here that the Presidential outcome was altered by hacking the BMDs. And Dr. Gilbert does not indicate any effort to determine the total number of spoiled ballots in Georgia's Presidential contest, which he presumably could have explored with State Defendants. Neither does he provide any basis to believe there were only 832 or fewer spoiled ballots. But suppose for the sake of argument that the Presidential election outcome in Georgia had been altered by hacking the BMDs, and there *were* complaints from the 832 voters that Dr. Gilbert has calculated. What then? It seems all but certain that these complaints would have been dismissed or drowned out in the cacophonous aftermath of the election or simply disregarded by election workers at the polling sites as voter errors. Yet the official count, the risk-limiting audit, and the recount would all have found the wrong winner, and there would be no

way to recover any altered vote or correct the election outcome short of rerunning the election. With a mere 832 complaints among 5 million participating voters (amidst a sea of other complaints, real and imagined), it is unlikely that poll workers or election officials, including State Defendants, would realize or even suspected there was a systemic problem with the BMDs, and it is completely implausible that they would take the drastic but necessary step of asking Georgians to vote again. Georgia's election system is susceptible to this extraordinary risk as long as it remains vulnerable to the attacks I described in my report (and potentially others).

21. To get to the point of making a decision to rerun an election, State Defendants (among others, perhaps) would first need to know how many voters discovered a problem when verifying their ballots. As Dr. Gilbert points out, the number of spoiled BMD ballots provides an upper bound on the number of voters who discovered and corrected an error (¶ 12). He does not say how many spoiled ballots there actually were in November 2020. If State Defendants knew the number was less than 832, they likely would have shared this fact with Dr. Gilbert, and he would have stated it in his report. It is reasonable to infer that either there were more than 832 spoiled ballots (and the attack is plausible) or State Defendants *do not know* how many BMD ballots were spoiled during the election, eight months later, despite

what Dr. Gilbert acknowledges those ballots would suggest about the reliability of the election.

22. That State Defendants may not know this information is consistent with gaps in other important election data that Georgia counties report to the Secretary of State. State Defendants recently produced electronic data (election projects) that I understand were required to be returned to them by counties after the November 2020 and January 2021 elections. In both elections, a large fraction of counties failed to return any data, returned the wrong data, or omitted data necessary for assessing the security and integrity of the result, such as election databases or ballot images. More than six months after these elections, the Secretary of State has not been able to assemble these electronic records and has not indicated any effort or willingness to do so. Yet the only way that State Defendants could use the number of spoiled ballots as a defense against BMD-based cheating would be if the poll workers accurately tracked it, counties accurately aggregated it, and the Secretary's Office received such data from across the state before the election result was determined. Even then, it is unlikely that the Secretary would be prepared to react by *rerunning the election* if the number of spoiled ballots exceeded the number predicted in an outcome-changing attack.

23. Given the ineffectiveness of such defenses and the critical security problems in Georgia's BMDs, I (like Dr. Appel) recommend that BMDs be reserved for voters who need or request them, as is the case in most states. Dr. Gilbert responds by claiming, without evidence, that "[d]isabled voters are even less likely to identify an error on their printed ballot" (¶ 14). I am unaware of any study that supports this sweeping indictment of voters with disabilities, which encompasses a vast array of disabilities that would not impact the ability of the voter to identify an error on their printed ballot in any way. He also contends that blind voters cannot detect errors on their ballot at all, but this is not true. Many blind voters use assistive technology to read printed text and likely could do so to verify their ballots. Moreover, only some voters who need BMDs are blind. For instance, those with motor impairments that prevent them from marking a ballot by hand would not necessarily have any greater difficulty verifying the printed text than any other voter. In any case, if BMDs are used primarily by voters with disabilities (as in most jurisdictions that use BMDs), they will represent a *much* smaller target,[7] and an

[7] Although Dr. Gilbert cites a figure that would imply that 10% of Georgians who voted in 2020 were disabled, data from Maryland, where BMDs are available upon request, suggests that only about 1.8% of voters would request to use BMDs if they were offered a hand-marked ballot first. (*Halderman decl.*, Aug. 19, 2020, Dkt. 785-2 at 49.) Dr. Gilbert's citation to the number of all Georgia voters with disabilities is highly misleading since, again, very few of those voters would be

outcome-changing attack on any given election will be detectable with a much lower rate of voter error detection than when all in-person voters use BMDs as they do in Georgia today. This in turn creates a strong disincentive for bad actors to attempt hacking an election (the risk likely is not worth the reward when the outcome is highly unlikely to be changed), which means individual votes would be less likely to be altered by hacking.

24. In his only direct response to my expert report, Dr. Gilbert states that he is not aware that I have "provided equipment marred by 'undetectable' hacks to any other independent researcher" (¶ 15).[8] This is a curious and ironic criticism coming from Dr. Gilbert, since he evidently chose not to evaluate my findings through an examination of the voting equipment himself, which he does not explain. Moreover, Dr. Gilbert misreads my report. It does not claim that malicious software infecting a BMD would be undiscoverable by any possible means. If an individual BMD is

unable to vote on a hand-marked paper ballot, consistent with the number reported in Maryland.

[8] Dr. Gilbert ignores that, as I understand it, State Defendants have objected to my report and the underlying work being shared with third parties (except Dominion), including other independent researchers, with whom I am eager to share my work for review. I am confident in my findings and believe they should be shared promptly with appropriate election security researchers and officials in an effort to mitigate the critical vulnerabilities in Georgia's voting equipment that I describe. I invite Dr. Gilbert to join me in seeking State Defendants' consent to do that.

*known* to contain malware, there will likely be some level of detailed forensic scrutiny that can detect where the malware is, perhaps requiring months of expert analysis per machine at extraordinary expense. It would be completely infeasible to perform this level of analysis on every machine before every election, much less between an election and the deadline for certification of its results. (And after manipulating ballots, malware could remove all traces of its presence from a machine, defeating any possible post-election examination of the device.) What my report shows is that vote-stealing malware of the type I have constructed would not be detected by any of the defenses that State Defendants purport to practice. I describe in detail how such malware would defeat QR code authentication, logic and accuracy testing, on-screen hash validation, and external APK validation (as was used by Pro V&V after the November election). Dr. Gilbert offers no rebuttal to these findings. He does not dispute them or even address them.

25. Moreover, there is already an example of an "undetectable" attack entered into testimony: exploitation of the Drupal vulnerability discovered by Logan Lamb in the Center for Election Systems server. As Lamb attested, the developers of the primary tool for detecting this vulnerability stated that "[n]either [the defensive tool] nor an expert can guarantee a website has *not* been compromised. They can only

confirm with certainty a website *has* been compromised."[9] Furthermore, the Drupal developers state that any server running the vulnerable software after the initial disclosure of the vulnerability should be assumed to have been compromised unless it was patched within *hours* of disclosure. According to the timeline presented in Lamb's declaration, he found the KSU server to be in a vulnerable state on August 28, 2016, nearly two years after the initial announcement of the critical vulnerability (October 15, 2014).[10] The KSU server image also contains evidence that a second vulnerability, the so-called Shellshock flaw, was exploited on December 2, 2014.[11] This vulnerability was publicly disclosed more than two months earlier and widely publicized in the media as a critical vulnerability, yet the KSU server remained unpatched.

26. An attacker who compromised the KSU server could therefore have maintained undetected access to the compromised server. Since the server remained in a vulnerable state undetected for almost two years, it is highly likely that it was successfully attacked at some point in time. An attacker who did so would have been able to move laterally to other systems within the CES network and to other

[9] *Lamb decl.*, Dkt. 258-1 at 19.

[10] See "Drupal Core - Highly Critical - Public Service announcement" (Oct. 29, 2014), available at https://www.drupal.org/PSA-2014-003.

[11] *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 23.

components of Georgia’s voting system. As I have previously pointed out, many election system components that could have been compromised in this way are still in use in Georgia today, where they provide a means by which attackers could spread vote-stealing malware to the BMDs.

27. Rather than address the many threats to Georgia’s voting system, Dr. Gilbert persists in drawing illogical comparisons between BMDs and hand-marked paper ballots. For instance, he questions why Plaintiffs have presented no research “regarding voters’ proclivity to review [hand-marked paper ballots] to ensure their ballots are marked and will count as intended” (¶ 8). Much like Dr. Gilbert’s earlier testimony that “[i]n essence, a BMD is nothing more than an ink pen,”[12] one does not need expertise in election security to find fault with this reasoning. Preventing voters from making accidental mistakes is a completely different problem from preventing their selections from being deliberately and systematically changed by an attacker who has compromised the BMDs. There is abundant evidence that voters do sometimes make errors whether filling out a ballot by hand or by machine. Bad ballot design exacerbates this problem with both voting modalities, but following ballot design best practices can greatly reduce it. Both

[12] *Gilbert decl.*, Dkt. No. 658-3 at 60.

BMDs and scanners that count hand-marked ballots can also be configured to reject overvotes and to warn voters about undervotes, the most common kinds of voter errors. Moreover, unlike older technologies for counting hand-marked ballots, the scanners used in Georgia (when properly configured) can detect improperly or incompletely marked bubbles and present them to human operators to adjudicate whether the marks should count as votes. Election officials can use all of these options to help protect voters from their own mistakes, but none of them offers protection against a BMD that deliberately changes the selections printed on a voter's ballot (or those encoded in the ballot barcode). The central problem with Georgia's highly vulnerable BMD system—that attackers can change all records of the voter's intent without being detected by election officials—has no parallel in a hand-marked paper ballot system.

28. Dr. Gilbert concludes as he started, with vague and sweeping generalities. "Simply put, BMD elections systems are no more insecure than [hand-marked] systems" (¶ 16). It is unclear whether he is claiming that *all* BMD systems are at least as secure as all hand-marked systems or merely that some specific BMD system (such as the one he recently developed himself to address some of the reliability problems that exist with Georgia's BMDs) is at least as secure as some hand-marked system, but this is of little consequence. The only BMD system that is

relevant here is the Dominion ICX as used in Georgia. As my expert report details, Georgia's BMD system suffers from numerous, severe vulnerabilities. These vulnerabilities would have little potential to change election outcomes if use of BMDs were limited to voters who need or request them, as Curling Plaintiffs desire, and they would be far less likely to affect the personal votes of individual Georgia voters.

**Reply to Declarations of Dr. Benjamin Adida**

29. The declarations by Dr. Adida that State Defendants have submitted predate my expert report, so Dr. Adida's opinions are not informed by the critical vulnerabilities in Georgia's BMD equipment that my analysis has revealed or by anything else in my lengthy, detailed report. Nor are they informed by any events that occurred in the year since he first provided these declarations, such as any aspect of the November 2020 election in Georgia or the Secretary of State's study indicating that few voters verified their respective ballots in that election.

30. Nevertheless, Dr. Adida's first declaration is correct that "Running a risk-limiting audit is one of the most important advances states can take in improving election integrity—without an RLA, we are effectively trusting computerized scanners to count our paper ballots" (Dkt. 834-2 at ¶ 5). This is true, but, as my expert report shows, without a risk-limiting audit Georgia is also trusting its critically

vulnerable BMDs to generate ballots with QR codes that correctly reflect voters' selections. Obviously compromised BMDs and compromised scanners could change individual votes and election outcomes. But again, nothing suggests that Georgia's scanners suffer from such easily exploitable critical vulnerabilities as the BMDs do.

31. Dr. Adida and I also agree that RLAs are important for discovering whether compromised BMDs have manipulated enough ballot QR codes to change the outcome of an election (¶ 12). Although RLAs are, as Dr. Adida says, "of the utmost importance" (¶ 6), Georgia does not require an RLA in the vast majority of elections and the vast majority of contests, leaving both election outcomes and individual voters' votes susceptible to manipulation via BMD malware. Additionally, it is insufficient for states to merely (in Dr. Adida's words) "take meaningful steps to implement RLAs"; rather, states have to *actually conduct* reliable RLAs, which Georgia does not intend to do for the vast majority of its elections (or perhaps any of its elections, depending on the reliability of the audit procedures it implements).

32. In his second declaration, Dr. Adida refers to a "dispute amongst academics regarding whether voters verify their ballots using ballot-marking devices" (Dkt. 912-1 at ¶ 11). This statement reflects a misunderstanding of the state of research today. I am not aware of any scientific research that supports the proposition that Georgia voters would likely detect more than a small fraction of

errors caused by BMD malware. In contrast, the past two years have seen a wave of laboratory studies and multiple field observation studies addressing this question, all of which strongly indicate the opposite, that few voters carefully review their ballots and so the vast majority of errors caused by BMD malware would likely to go undiscovered and uncorrected. Although there once was uncertainty about whether most voters carefully verify their BMD ballots, there is no longer any serious scientific dispute that they do not. It is the hallmark of good science (and of good public policy) that it evolves based on new evidence, such as the University of Georgia study commissioned by the Secretary of State that I discussed above—which Dr. Adida has not addressed.

33. Georgia's election system needs to evolve as well. Due to the critical vulnerabilities in Georgia's BMDs that are described in my expert report, Georgia voters face an extreme risk that BMD-based attacks could manipulate their individual votes and alter election outcomes. Even in the rare contests for which the State requires a risk-limiting audit, the scientific evidence about voter verification shows that attackers who compromise the BMDs could likely change individual votes and even the winner of a close race without detection. Georgia can eliminate or greatly mitigate these risks by adopting the same approach to voting that is practiced in most of the country: using hand-marked paper ballots and reserving

BMDs for voters who need or request them. Absent security improvements such as this, it is my opinion that Georgia's voting system does not satisfy accepted security standards. Neither Dr. Gilbert nor Dr. Adida offers a contrary opinion in their respective declarations, instead ignoring the critical issue of whether the *voting system used in Georgia*—which neither claims to have examined—reliably protects the right to vote for individual Georgia voters.

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 August, 2021 in Rushland, Pennsylvania.

______________________________________
J. ALEX HALDERMAN

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

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

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

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

## LIMITED MOTION TO INTERVENE BY R. KYLE ARDOIN, in his official capacity as the LOUISIANA SECRETARY OF STATE

Pursuant to Rule 24(b), the Louisiana Secretary of State, R. Kyle Ardoin, in his official capacity (the "LA Secretary of State") respectfully moves to intervene for the limited purpose of seeking access to a report sealed in this litigation.

The Plaintiffs filed under seal a report by noted cybersecurity expert, Dr. J. Alex Halderman. *See* Doc. 1126 (referencing service of report); Doc. 1130-1 (filing of report under seal); Doc. 1130-2 ¶ 7 (acknowledging contents of report remains confidential). Based on public filings and statements by Dr. Halderman in his declarations, including direct references to Louisiana and its election equipment, it appears that the contents of Dr. Halderman's report bear directly on the equipment currently used by the state of Louisiana for early voting.

The LA Secretary of State is the "chief election officer of the state." La. Const. Art. 4 § 7. The information contained in Dr. Halderman's sealed July 1, 2021. report appears to directly address the Dominion ICX machines Louisiana uses to conduct early voting in the state. As the chief election officer, the LA Secretary of State is obligated to investigate potential cybersecurity vulnerabilities with the Dominion ICX system, including those currently addressed in Dr. Halderman's sealed report. The LA Secretary of State takes no other positions in this litigation and it does not otherwise seek to align with any of the parties or assert any claims or defenses.

In accordance with the procedures set forth by the Court, the LA Secretary of State seeks to intervene for the limited purpose of accessing Dr. Halderman's report. The LA Secretary of State will agree to the terms of the Court's Protective Order (Doc. 477) and take such other steps as are necessary to limit the review of this report, including limiting who may view it and maintaining custody of the report in accordance with the Protective Order. Wherefore, the LA Secretary of State requests that its Limited Motion to Intervene be granted.

Respectfully submitted,

______________________________
Chad V. Theriot

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

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

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

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

# MEMORANDUM IN SUPPORT OF LIMITED MOTION TO INTERVENE BY R. KYLE ARDOIN, in his official capacity as the LOUISIANA SECRETARY OF STATE

The Louisiana Secretary of State, R. Kyle Ardoin, in his official capacity, (the "LA Secretary of State") submits this memorandum in support of its Limited Motion to Intervene. As will be demonstrated below, the LA Secretary of State has a compelling interest in accessing the sealed July 2021 report filed by Dr. J. Alex Halderman in this litigation. The LA Secretary of State will be able to maintain the confidentiality of this report, and this limited intervention will not retard or otherwise disrupt the progress of this litigation.

## Factual Background

Following an analysis conducted by Dr. Halderman, his July 1, 2021, expert report details multiple potential security flaws in the Dominion ICX ballot marking device machines, including possible vulnerabilities that could permit attackers to install malicious software on the voting system. The State of Louisiana also uses the Dominion ICX system for its early voting. Dr. Halderman references this report in a September 21, 2021, declaration filed with the Court (Doc. 1177-1, page 1). However, the underlying report has been designated as Confidential under the Court's Protective Order (Doc. 477). According to Dr. Halderman's declaration, the Dominion ICX machine could also contain other possible critical flaws that have yet to be discovered. (Doc. 1177-1, page 2)

In his declaration, Dr. Halderman also acknowledges the findings in his report have implications outside of Georgia. Specifically, Dr. Halderman mentions Louisiana's own use of the Dominion ICX machines for early voting. (Doc 1177-1, page 3). Further, he acknowledges that the lack of access to his analysis may impair the ability of states such as Louisiana to take action on the potential vulnerabilities he identified in ICX machines, including updating software and making changes to procedures: "Continuing to conceal those problems from those who can-and are authorized to-address them, to the extent possible, serves no one and only hurts voters (and heightens the risk of compromise in future elections)." (Doc. 1177-1, page 3)

Dr. Halderman's declaration makes clear that informing responsible parties about the ICX's potential vulnerabilities is becoming more urgent by the day. (Doc.

1177-1, page 4) Further, Court records also support the fact that the level of analysis and investigation by Dr. Halderman, and other experts, of the Dominion ICX voting system has never occurred previously. Another expert, Dr. Hursti, points out "[t]o my knowledge, no jurisdiction has permitted, and Dominion has not permitted, independent research, academic or otherwise, to be conducted on its systems, which greatly limits the number of people with any experience with the Dominion systems." (Doc. 964, page 47) Given the likelihood that no other detailed analysis of these machines is available to the LA Secretary of State, Louisiana has a critical and timely interest in this specific report. Access to Dr. Halderman's report would enable Louisiana to review his findings, and possibly mitigate some of these potential vulnerabilities in connection with the upcoming 2022 elections.

## REQUESTED RELIEF

This motion seeks access to the July 1, 2021, report by Dr. Halderman of his analysis of the Georgia election system, as referenced above. Currently, this report is deemed Confidential under this Court's Protective Order (Doc. 477).

At this time, Louisiana is one of sixteen states that use the Dominion ICX voting system. The state currently leases 780 ICX machines to conduct early voting in each election. Dr. Halderman specifically identifies Louisiana as one of the states at risk from the potential cybersecurity threats discovered contained in his report and referenced in his September 21, 2021, filed declaration. (Doc. 1177-1, page 3).

The findings in Dr. Halderman's report appear to address potential cybersecurity flaws and vulnerabilities with the machines which, if exploited, could potentially overthrow the intent of the voter. In the additional declaration filed by Dr. Halderman in September 2021, it is made clear that the report has implications outside of the state of Georgia and its use of the ballot marking device function but broadly to include the Dominion ICX voting system as a whole. (Doc. 1177-1, pages 2-3)

The contents of this report remain under by seal by this Court. The Secretary seeks access to this report for purpose of discovering unknown potential vulnerabilities and taking the requisite mitigation measures and procedural steps to address any potential security flaws discovered in the Dominion ICX voting system used by Louisiana for its early voting. The request for this information is time sensitive and critical to conducting early voting in the state in light of the upcoming 2022 elections and recent legislative changes.

Louisiana will hold elections in spring of 2022. Municipal elections will be held on March 26, 2022, for the primary election and April 30, 2022, for the general election. Early voting will begin on March 12, 2022, for the primary election and

April 16, 2022, for the general election, with some limited early voting taking place prior to those dates for nursing home residents.

In the fall of 2022, the state of Louisiana will conduct elections in accordance with the federal election date of November 8, 2022, with early voting scheduled for beginning on October 25, 2022. The state will hold a general election on December 10, 2022, with early voting beginning on Saturday, November 26, 2022, with limited early voting taking place prior to those dates for nursing home residents.

Access to this report is also critical to conform to the legal requirements recently enacted by the Louisiana legislature, which established a voting system commission "to further the preservation of democracy by strengthening the state's commitment to maintaining the faith, integrity, and trust in election, voting, and ballot-counting processes, to provide the highest level of election security and functionality ." (La. R.S. 18:1362.1(A)(2)). As the commission is tasked with making a recommendation to the LA Secretary of State for any new voting system or equipment to be used in Louisiana, it is necessary that the LA Secretary of State is fully-informed of any potential cybersecurity concerns or exposures with its current system as the state moves forward to evaluate and ultimately procure a new voting system. The independent and impartial expertise provided in this report is invaluable to the state in identifying voting systems that encapsulate the requirements set forth by the legislature to provide the highest level of security and functionality as well as upholding public trust in the process. This information would remain subject to confidentiality by the LA Secretary of State pursuant to the terms of any signed Acknowledgement and Agreement to Be Bound (Exhibit A, Doc. 477, page 19).

The LA Secretary of State asks that the Court recognize the urgent need for Louisiana to avail itself of critical cybersecurity information related to the security and integrity of voting for the LA Secretary of State to address any possible threats and vulnerabilities in the Dominion ICX machines, in advance of the spring and fall 2022 elections and in compliance with the recently enacted requirements by the Louisiana legislature.

## ARGUMENT

### I. The Louisiana Secretary of State should be allowed to intervene for the limited purpose of accessing the report.

Pursuant to Federal Rule of Civil Procedure 24(b) a court may grant permissive intervention if three conditions are met: (1) movant must show an independent ground for jurisdiction; (2) motion must be timely; and (3) claim must have a claim or defense and main action must have a question of fact or law in common. *Johnson v. Mortham,* 915 F.Supp. 1529 (N.D. Fla. 1995). Courts generally construe this provision broadly. *United States ex rel. McGough v. Covington Techs.*

*Co.,* 967 F.2d 1391, 1394 (9th Cir. 1992). However, in this instance the state of Louisiana is only seeking a limited intervention to receive access to judicial records and not be made a party to the litigation. Given this limited purpose, Rule 24(b) dictates only that the motion be timely. *E.g., Beckman Indus., Inc. v. International Ins. Co.*, 966 F.2d 470, 473–74 (9th Cir. 1992).

The LA Secretary of State's motion is timely, satisfying the four relevant factors "(1) the period of time during which the putative intervenor knew or reasonably should have known of his interest in the case before he petitioned for leave to intervene; (2) the degree of prejudice to the existing parties as a result of the would-be intervenor's failure to move to intervene as soon as he knew or reasonably should have known of his interest; (3) the extent of prejudice to the would-be intervenor if his position is denied; and (4) the presence of unusual circumstances militating either for or against a determination that the application is timely." *Walker v. Jim Dandy Co.,* 747 F.2d 1360, 1365 (11th Cir.1984).

While the litigation in this present case has been ongoing since 2017, the issue of potential cybersecurity vulnerabilities with the Dominion ICX machines ballot marking device voting system was brought before the Court in 2020. (Doc. 964, pages 2-3) More recently, however, in September 2021, Dr. Halderman's filing before the Court raised possible concerns with the Dominion ICX system, noting that it is likely to contain other flaws, and specifically named Louisiana as one of the affected states. (Doc. 1177-1, page 3). Further, Dr. Halderman noted the urgency for states to access the information in order to address potential flaws through mitigation efforts as well as procedural changes.

It has been a little over two months since that declaration was filed with the Court and Louisiana was specifically identified. (Doc. 1177-1). This motion will not prejudice nor delay any subsequent motions filed by either the Plaintiffs or Defendants in this case. This motion is intending only to provide limited access to information in Dr. Haldeman's report to the LA Secretary of State, which is already accessible to both parties. Denying this limited intervention would be extremely detrimental to the state of Louisiana. The state of Louisiana is seeking intervention only as to protect its early voting system from identified potential security vulnerabilities. In order to do so, it must be allowed to see the information contained in the report, as referenced by Dr. Halderman. (Doc. 1130-1; Doc. 1177-1). Further, the fact that the state will be conducting elections in both the spring and fall of 2022 only heightens the need that this motion is timely and the release of that information is extremely time-sensitive.

## II. Under the presumption of the common law right-of–access to Court records, the LA Secretary of State is permitted to view the report.

Courts have long recognized the presumption of public access to judicial documents. *Callahan v. United Network for Organ Sharing,* 2021 U.S. App. LEXIS 34201; 2021 WL 5351863, __ F.4th __ (11th. Cir. Nov. 17, 2021). Courts have held that access is "an essential component of our system of justice" and "instrumental in securing the integrity of the process." *Id. (quoting Chi. Trib. Co. v. Bridgestone/Firestone, Inc.*, 263 F.3d 1304, 1311 (11th Cir. 2001)*).* This right attaches to judicial records and the contents of Dr. Halderman's July 1, 2021, report "were used in connection with merits briefing such that the public right of access attaches." *Callahan v. United States HHS*, 2020 U.S. Dist. LEXIS 204550 (N.D. Ga., Sept. 29, 2020). His report and in-depth analysis of the Dominion ICX voting machines and potential security flaws and vulnerabilities are a critical component to the Plaintiffs' argument.

This presumption of access is not absolute, so Courts must determine whether good cause exists, balancing the interests of one party to keep the information confidential and the other party's right of access. *See Romero v. Drummond Co., Inc.*, 480 F.3d 1234, 1246 (11th Cir. 2007). The Court looks at a number of factors in weighing the competing interests, including "whether allowing access would impair court functions or harm legitimate privacy interests, the degree of and likelihood of injury if made public, the reliability of the information, whether there will be an opportunity to respond to the information, whether the information concerns public officials or public concerns, and the availability of a less onerous alternative to sealing the documents." *Id.*

The LA Secretary of State recognizes the importance of protecting against sensitive voter and cybersecurity information being widely disseminated to the public. However, Louisiana's need for access to Dr. Halderman's report is distinguishable from a public interest, and Louisiana's proposal for limiting its access and protecting the report more than satisfies any concern about unwarranted disclosure. The LA Secretary of State continues to employ the Dominion ICX voting systems in conducting early voting in the Louisiana. It is absolutely necessary to address any and all potential flaws with the machines prior to the spring of 2022 elections. The potential injury to over 3,000,000 voters in the state of Louisiana and the protection of their right to vote outweighs the fact that this information is currently only available to the parties in this litigation. A less onerous alternative in this situation is to grant access to the LA Secretary of State pursuant to this Court's Protective Order.

Further, Dr. Halderman, based upon his own findings, cites to this Court the need to make this information available to interested parties:

> Public disclosure ensures that all jurisdictions that rely on the vulnerable equipment will be aware of the problems and able to begin mitigating them. It informs law enforcement and national security groups about forms of attack that they should be on the lookout for. It helps jurisdictions that are procuring new equipment make better informed purchases. It ensures that vendors of other equipment that may suffer from similar problems are on notice. (Doc. 1130-2, pages 1-2)

In balancing the interests of the parties here, the state of Louisiana should be afforded access to this information as it continues to be withheld from the public. To deny the state access to critical information regarding possible issues impacting their own election system is outside the scope of what this sealed information was intended to protect.

## III. The LA Secretary of State Will Comply With All Confidentiality Measures Set By This Court in Its Protective Order

Pursuant to the Minute Entry filed October 7, 2021, this Court set out narrow parameters in which it would consider disclosure of Dr. Halderman's report. (Doc. 1184, pages 1-2) By way of this motion, the LA Secretary of State is making a formal request for that information.

Pursuant to this Court's Protective Order (Doc. 477, page 8), the LA Secretary of State seeks limited disclosure of the sensitive information contained in Dr. Halderman's report for the reasons discussed above. The LA Secretary of State has read and agrees to sign the terms of the "Acknowledgement and Agreement to Be Bound" ("Exhibit A" Doc. 477, page 19) should this Court grant access to the report. The LA Secretary of State accepts full compliance with the terms laid out by this Court.

As chief election official, the LA Secretary of State's office has the necessary protocols and security measures in place to safeguard sensitive voter information, sensitive technology and equipment systems, and cybersecurity information. The state of Louisiana currently operates under similar agreements for the leasing of software, firmware, and hardware, maintaining the confidentiality required of such agreements with private entities. Further, this state has entered into data sharing information agreements with federal and state agency partners that maintain the requisite privacy protections and maintain that this information shall not be subject to disclosure under state public record law. (La. R.S. 44:4.1(b)(37); *see also* La. R.S. 44:1(b); *see also* La. R.S. 44:3.2; *see also* La. 18:154).

All data contained in the report shall be used by the LA Secretary of State exclusively for the purpose of addressing and mitigating potential vulnerabilities in the Dominion ICX machines used by the state, including any corresponding component or software of the voting system. The sharing of the report shall adhere to all applicable federal and state laws governing the confidentiality of the agreement. The state has established safeguards to protect the confidentiality of the data and limit access to the individuals named below. The confidential data will be stored in a place secure from any unauthorized access. The state will comply with any necessary reporting, storage, or disposal requirements to comply with the orders of this Court to safeguard the data.

The state also maintains that the information will be strictly limited in access with the Department itself, limited only to high-level officers who oversee the relevant elections, operations, and information and technology divisions, and only these authorized users shall have access to shared data for the purpose of addressing any potential vulnerabilities in the current operation of the Dominion ICX machines for early voting in the state of Louisiana. Louisiana law also requires cybersecurity training for key personnel (*see* La. R.S. 18:31). Access to the report shall be limited to the following individuals:

- The LA Secretary of State
- The First Assistant Secretary of State
- The Commissioner of Elections

- The Elections Program Administrator
- The Director of Information Technology
- The Chief Information Officer

## CONCLUSION

In closing, the LA Secretary of State takes very seriously the concerns noted by this Court:

> The Plaintiffs' national cybersecurity experts convincingly present evidence that this is not a question of "might this actually ever happen?" – but "when it will happen," especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, "we have never seen it," the future does not bode well. (Doc. 964, page 146)

For the foregoing reasons, the LA Secretary of State requests the Court grant the Limited Motion to Intervene and grant access to the report containing Dr. Halderman's analysis of the Dominion ICX voting system.

Respectfully submitted,

________________________________
Chad V. Theriot

## CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 5.1

The undersigned hereby certifies that the foregoing document has been prepared in accordance with the font type and margin requirements of Local Rule 5.1 of the Northern District of Georgia, using a font type of Times New Roman and a point-size of 14.

______________________________
Chad V. Theriot

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

| | | |
|---|---|---|
| DONNA CURLING, *et al.*,<br>Plaintiffs,<br>v.<br>BRAD RAFFENSPERGER, *et al.*,<br>Defendants. | :<br>:<br>:<br>:<br>: | CIVIL ACTION NO.<br>1:17-cv-2989-AT |

## **ORDER**

This matter is before the Court on R. Kyle Ardoin's Motion to Intervene in his Official Capacity as the Louisiana Secretary of State [Doc. 1243]. The Louisiana Secretary of State ("LA Secretary of State") seeks to intervene in this case for the limited purpose of obtaining access to a provisionally sealed report (Doc. 1131) issued by cybersecurity expert Dr. J. Alex Halderman on behalf of the Curling Plaintiffs.

In his motion, the LA Secretary of State argues that he has a compelling interest in accessing Dr. Halderman's report because it details multiple potential security flaws in Dominion ICX's ballot marking device machines, which the State of Louisiana utilizes for early voting. The LA Secretary of State emphasizes that in a subsequent declaration Dr. Halderman "specifically identifie[d] Louisiana as one of the states at risk from the potential cybersecurity threats." (Doc. 1243-1 at 3–4.) And he contends that "[a]ccess to Dr. Halderman's report would enable Louisiana to review his findings, and possibly mitigate some of these potential vulnerabilities in connection with the upcoming 2022 elections." (*Id.* at 3.)

In a response to the LA Secretary of State's motion, the State Defendants in this case argue that "Dr. Halderman's purported reference to the voting machines used for early voting in Louisiana is not a reason to grant Intervener's motion under Federal Rule of Civil Procedure 24(b)." (Doc. 1244 at 1–2.) Under Rule 24(b), "[o]n timely motion, the court may permit anyone to intervene who: (A) is given a conditional right to intervene by a federal statute; or (B) has a claim or defense that shares with the main action a common question of law or fact." Accordingly, the State Defendants contend, "Because [the LA Secretary of State] does not have a claim or defense that shares with the main action a common question of law or fact, permissive intervention under Rule 24(b)(1)(B) is not appropriate." (Doc. 1244 at 2.)

However, as the LA Secretary of State notes, courts have applied a more relaxed approach to Rule 24's requirements where, as in this case, the movant seeks to intervene for the limited purpose of requesting access to documents subject to a confidentiality order. For example, in *Beckman Industries, Inc. v. International Insurance Co.*, 966 F.2d 470 (9th Cir. 1992), the intervenors sought to intervene in the case for the limited purpose of modifying a protective order. Like the State Defendants here, the defendant in that case argued that the intervenors had failed to satisfy Rule 24's requirements for permissive intervention because they had failed to identify a claim or defense that was relevant to the action. *Id.* at 473–74. But the court found that "[t]here is no reason to require such a strong nexus of fact or law when a party seeks to intervene only for the purpose of modifying a protective order." *Id.* at 474. The court opined that "no independent jurisdictional basis" was required because the intervenors were not requesting that the court either rule on additional claims or make them parties to the action. *Id.* at 473. They were simply asking the court to exercise a power that it already had — "the power to modify the protective order." *Id.*; *see also* 7C Charles Allen Wright et al., Federal Practice and Procedure § 1917 (3d ed. 1998) ("A narrow exception to the rule that permissive intervention generally requires an independent jurisdictional basis is when a third party seeks to intervene for the limited purpose of obtaining access to documents protected by a confidentiality order.").

Similarly, in *E.E.O.C. v. National Children's Center, Inc.*, 146 F.3d 1042 (D.C. Cir. 1998), the court observed that "despite the lack of a clear fit with the literal terms of Rule 24(b)" in these circumstances, "every circuit court that has considered the question has come to the conclusion that nonparties may permissively intervene for the purpose of challenging confidentiality orders." *Id.* at 1045. Adopting a "flexible approach" toward permissible intervention under Rule 24, and recognizing the "longstanding tradition of public access to court records," the court construed the Rule as providing "an avenue for third parties to have their day in court to contest the scope or need for confidentiality." *Id.* at 1046 (internal quotations marks and citations omitted).

On the other hand, even under this more "flexible approach" to Rule 24, "permissive intervention is an inherently discretionary enterprise," and courts have discretion to deny motions to permissively intervene even when the requirements of Rule 24 are otherwise satisfied.[1] *Id.* at 1046–48. Notably for purposes of this case, the LA Secretary of State himself acknowledges "the importance of protecting against sensitive voter and cybersecurity information being widely disseminated to the public." (Doc. 1243-1 at 10.) And as the State Defendants point out, this Court has expressed significant concerns about disseminating the information contained in Dr. Halderman's report. In spite of these very real concerns, the LA Secretary of State argues that the common law right of public access and the potential injury to voters in the State of Louisiana outweigh any interest in preventing him from accessing Dr. Halderman's report. While the Court gives great weight to the right of public access to information filed on the docket and the public interest in information regarding elections, it is not persuaded under the specific circumstances presented here that the petitioners' intervention motion should be granted.

As the LA Secretary of State concedes, the common law right of public access is not absolute; the Court must also consider a number of competing interests that may weigh against disclosure. Those factors include "whether allowing access

[1] The Court takes no position on whether the LA Secretary of State's motion was timely.

would impair court functions or harm legitimate privacy interests, the degree of and likelihood of injury if made public, the reliability of the information, whether there will be an opportunity to respond to the information, whether the information concerns public officials or public concerns, and the availability of a less onerous alternative to sealing the documents." (*Id.* at 9–10) (citing *Romero v. Drummond Co., Inc.*, 480 F.3d 1234, 1246 (11th Cir. 2007)). The LA Secretary of State argues that a "less onerous alternative" would be granting him access to Dr. Halderman's report subject to the Court's Protective Order. However, the Court remains concerned about the risks associated with further dissemination of the report.[2] As the Court stated during a prior hearing in which the Coalition Plaintiffs sought to further disseminate the same report, "[a]s it is, I think that we're on very difficult territory." (Doc. 1143, Tr. at 66:25–67:1.) The Court still believes this to be true. Further disseminating Dr. Halderman's report presents complicated risks. Most importantly, sensitive information in the Report relating to the operation of Dominion's electronic voting software and system could potentially be misused by domestic or foreign hackers or alternatively used for other unlawful or improper purposes. At the current time, if the Court granted the LA Secretary of State access to Dr. Halderman's report, it could also open the floodgates to similar requests from other individuals and entities around the country, which would also increase the potential for hacking and misuse of

[2] The Court is not suggesting that the LA Secretary of State would intentionally fail to comply with the Protective Order if he were given access to Dr. Halderman's report.

sensitive, confidential election system information. Finally, as discussed below, the LA Secretary of State has other reasonable alternatives for assessing the sufficiency of its election system equipment.

For example, the LA Secretary of State could simply reach out to Dr. Halderman himself and request that Dr. Halderman perform a review of the State's election apparatus or Dominion systems on a retained basis. If anything, a targeted investigation of potential cybersecurity threats to Louisiana's own election system would more directly address the LA Secretary of State's concerns than a written report about the system utilized in Georgia. And even if as the LA Secretary of State argues, "the level of analysis and investigation by Dr. Halderman, and other experts, of the Dominion ICX voting system has never occurred previously," (Doc. 1243-1 at 3), that does not mean that a similar analysis and investigation could not be arranged in the future without the LA Secretary of State intervening in this case. In short, the LA Secretary of State has not established that intervening in this case for the purpose of accessing Dr. Halderman's report is an appropriate means of addressing concerns that actually fall within the scope of the LA Secretary of State's authority to investigate the functionality and any vulnerabilities in Louisiana's election system. Such concerns would be more appropriately addressed by retaining Dr. Halderman and other similarly skilled election cyber engineering experts.

The Court has carefully balanced the factors at play in reviewing the LA Secretary of State's intervention request. Given the particular circumstances and alternatives discussed in this Order as well as consideration of the briefs and factors discussed, the Court **DENIES** the LA Secretary of State's Motion to Intervene [Doc. 1243].

**IT IS SO ORDERED** this 10th day of January, 2022.

**Honorable Amy Totenberg**
**United States District Judge**

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

| | | |
|---|---|---|
| DONNA CURLING, ET AL., | ) | |
| | ) | |
| Plaintiffs, | ) | |
| | ) | |
| v. | ) | Civil Action File No.<br>1:17-CV-02989-AT |
| | ) | |
| BRAD RAFFENSPERGER, ET AL., | ) | |
| | ) | |
| Defendants. | ) | |

## MEMORANDUM IN SUPPORT OF MOTION TO INTERVENE FOR LIMITED PURPOSES

Fox News Network, LLC (“FNN”) seeks to intervene in this lawsuit pursuant to Federal Rule of Civil Procedure 24 for the limited purpose of obtaining access to a document kept under seal pursuant to the Court’s protective order. As demonstrated below, FNN has a substantial interest in obtaining access to the sealed expert report of Dr. J. Alex Halderman (submitted July 1, 2021) because it addresses questions that are common to a claim or defense in a separate action in which FNN is a defendant. Specifically, Dr. Halderman’s report is the result of his thorough analysis of the Dominion voting system used in Georgia in the 2020 election, and FNN is the defendant in a lawsuit brought by Dominion in which Dominion has relied upon Dr. Halderman’s expertise for the proposition that no votes were changed through a Dominion voting system in the 2020 elections. Compl. ¶ 68, *U.S. Dominion, Inc. v. Fox News Network, LLC*, No. N21C-03-257 EMD (Del. Superior Court Mar. 26, 2021) ("*Dominion v. FNN*") (alleging that "Professor J. Alex Halderman, the Director of the University of Michigan's Center for Computer Security & Society . . . told [FNN] explicitly, 'There is absolutely no evidence, none, that Dominion Voting Machines changed any votes in this election.'"). FNN should be permitted access to Dr. Halderman's expert report, *inter alia*, to determine the extent to which it contradicts his purported statement to FNN.

Accordingly, FNN is entitled to intervention as of right. *Comm'r, Alabama Dep't of Corr. v. Advance Loc. Media, LLC*, 918 F.3d 1161, 1173 (11th Cir. 2019) (upholding intervention as of right in similar case). At a minimum, FNN is entitled to permissive intervention. *E.g.*, *id.* at 1171 (courts may "exercise discretion" to grant permissive intervention when the moving party has a "claim or defense that shares with the main action a common question of law or fact," if intervention will not "unduly delay or prejudice the adjudication of the original parties' rights") (quoting Fed. R. Civ. P. 24(b)(3)); *accord Georgia Aquarium, Inc. v. Pritzker*, 309 F.R.D. 680, 690 (N.D. Ga. 2014) (describing a court's two-step inquiry as (1) whether the intervenor's claim or defense shares common questions of law or fact with the pending case and (2) whether the court should exercise its discretion to allow the intervention); *see also Athens Lumber Co. v. Fed. Election Comm'n*, 690 F.2d 1364, 1367 (11th Cir. 1982).

## BACKGROUND

Dr. Halderman is a retained expert in this case who was given access to certain Dominion hardware and software in order to perform a "technical and security analysis" of the Dominion voting system because "the issues covered by such [an] analysis fall within the heartland of this lawsuit's serious claims." Doc. 858 (Order Sept. 2, 2020). Dr. Halderman performed a twelve-week analysis of the Dominion system he was provided and generated a 25,000-word expert report. *See* Rebuttal Decl. of J. Alex Halderman ¶ 4 (Aug. 2, 2021) ("Halderman Rebuttal Decl."). That expert report has been filed under seal, and FNN understands that it remains designated Attorney's Eyes Only. *See* Doc. 1130-1 (filing of report under seal); Doc 1130-2 ¶ 7 (recognizing that contents of the report will remain under seal); Doc. 858 (Order requiring that access to and testing of Dominion software and hardware is subject to the protective order in this case); Doc. 477 (protective order).

Dr. Halderman has since submitted declarations in this case that are publicly available and that indicate Dr. Halderman's analysis uncovered multiple security problems with the Dominion system. Decl. of J. Alex Halderman, Doc. 1177-1 ¶ 1 (Sept. 21, 2021) ("Halderman Decl.") (stating that his "July 1, 2021 [sealed] expert report describes numerous security vulnerabilities" in the Dominion system utilized in Georgia elections, and warning that these flaws "are not general weaknesses or theoretical problems, rather specific flaws in [Dominion's] ICX software . . . that can [be] exploit[ed] to steal votes on ICX devices"); Halderman Rebuttal Decl. ¶ 2 (expressing similar concerns regarding the "numerous, critical vulnerabilities" with the Dominion system that he was permitted to examine).

FNN seeks to intervene for the limited purpose of obtaining access to Dr. Halderman's complete expert report.

FNN is the defendant in a defamation suit that Dominion filed in Delaware. *See* Compl., *U.S. Dominion, Inc., et al., v. Fox News Network, LLC*, No. N21C-03-257 EMD (Del. Superior Ct. Mar. 26, 2021) ("*Dominion v. FNN*"). Dominion alleges, *inter alia*, that FNN defamed Dominion by reporting on and repeating allegations made by President Trump and his legal team that Dominion voting systems are not secure and that Dominion systems' vulnerabilities contributed to fraud during the 2020 presidential election. *See generally id.* Dominion argues in that litigation that its defamation claim turns not on whether FNN truthfully reported the newsworthy allegations made by the president and his representatives (FNN's view) but on whether the underlying allegations about Dominion's voting systems were in fact true. *See generally id.* The Delaware litigation remains in the early stages, and the trial court there recently denied FNN's motion to dismiss (on Dec. 16, 2021), explaining in several places that at "the pleadings stage" factual issues must be resolved in Dominion's favor and that, in that court's view, FNN's dismissal arguments were affirmative defenses (including neutral reportage and fair-report doctrine) for which FNN may develop facts in support as the case proceeds. *See, e.g.*, Order at 44, *Dominion v. FNN*.

Accordingly, whether the Dominion systems in use in Georgia and elsewhere during the 2020 election were susceptible to manipulation or fraud—an issue that appears to have been thoroughly examined by Dr. Halderman—is a critical factual inquiry that FNN must continue to explore in its defense in the Delaware litigation. Notably, Dr. Halderman recognized that the security flaws he has uncovered suggest that there are additional, "equally critical flaws that are yet to be discovered." Halderman Decl. ¶ 4. Finally, Dr. Halderman has indicated that he will not disclose his report to others while the report remains subject to the protective order and AEO designation. Halderman Decl. ¶ 10 ("I of course have complied, and will continue to comply, with all directives from the Court regarding disclosure of my work in this matter.").

## SPECIFIC RELIEF REQUESTED

FNN seeks:

(1) intervention on a limited basis pursuant to Federal Rule of Civil Procedure 24 and

(2) entry of an Order granting FNN access to Dr. Halderman's July 1, 2021, expert report, which would be limited to 6 attorneys and consulting experts. FNN agrees to, and will abide by, the confidentiality requirements previously ordered by the Court in its protective order (Doc. 477).

## ARGUMENT and AUTHORITIES

### I. The Standards for Intervention under Rule 24 Generally Permit Timely, Limited Interventions for the Purpose of Obtaining Access to Sealed Documents

Courts in this circuit and across the country have granted intervention "for the limited purpose of seeking access to materials that have been shielded from public view either by seal or by a protective order." *EEOC v. Nat'l Children's Ctr., Inc.*, 146 F.3d 1042, 1046 (D.C. Cir. 1998); *id.* at 1045 ("[C]ourts have been willing to adopt generous interpretations of Rule 24(b) because of the need for 'an effective mechanism for third-party claims of access to information generated through judicial proceedings.'") (quoting *Public Citizen v. Liggett Grp., Inc.*, 858 F.2d 775, 783 (1st Cir. 1988)); *In re Alexander Grant & Co. Litig.*, 820 F.2d 352, 354 (11th Cir. 1987)

("[A]ppellants have standing to intervene in this action and challenge the propriety of the district court's protective order.") (citation omitted); *In re Midland Nat. Life Ins. Co. Annuity Sales Pracs. Litig.*, 686 F.3d 1115, 1120 (9th Cir. 2012) (upholding intervenors' right to access documents relevant to intervenor's separate, ongoing litigation); *see also* 7C Charles Alan Wright & Arthur R. Miller, Federal Prac. and Proc. Civ. § 1911 (3d ed. 2007) ("[C]ourts generally have interpreted their discretion . . . broadly and have held that it can be invoked by nonparties who seek to intervene for the sole purpose of challenging confidentiality orders.").

More specifically, the Eleventh Circuit has held that intervention for the purpose of accessing documents relevant to other litigation is proper. For example, in *Brown v. Advantage Engineering Inc.*, Amco Chemical reached a settlement agreement with a plaintiff, but negotiated that the agreement would be sealed. 960 F.2d 1013, 1015 (11th Cir. 1992). In an unrelated action, a separate plaintiff sued Amco Chemical and sought the settlement agreement from the prior suit, contending that the requested documents reportedly contained admissions from Amco that could prove helpful in the unrelated suit. *Id*. at 1015. The district court denied the motion to intervene, but the Eleventh Circuit reversed, noting that "trials are public proceedings" and "[o]nce a matter is brought before a court for resolution, it is no longer solely the parties' case, but also the public's case." *Id*. at 1016.

The Eleventh Circuit held that the "disclosure of sensitive information" is an insufficient basis to restrict disclosure of the information, but rather, "it must be shown that the denial is *necessitated by a compelling governmental interest, and is narrowly tailored to . . . that interest.*" *Id*. at 1015-16 (citing *Wilson v. American Motors Corp.*, 759 F.2d 1568 (11th Cir. 1985)). "Absent the showing of extraordinary circumstances . . . the court file must remain accessible to the public" and cannot remain "improperly sealed." *Id*. at 1016; *see also Wilson v. American Motors Corp.*, 759 F.2d 1568, 1570-71 (11th Cir. 1985) ("Simply showing that the information would harm the company's reputation is not sufficient to overcome the strong common law presumption in favor of public access.") (internal citation and quotations omitted).

## II. FNN Satisfies the Requirements of Rule 24, and the Court Should Exercise its Discretion to Grant the Requested Limited Intervention

In cases like this, the Eleventh Circuit has upheld both interventions as of right and permissive intervention. *E.g.*, *Advance Loc. Media*, 918 F.3d at 1173. Most importantly, "[i]ntervention under either Rule 24(a) or 24(b) must be timely filed." *Id.* at 1171.

Under Rule 24(a), courts must grant intervention as of right when someone "claims an interest relating to the property or transaction that is the subject of the action, and is so situated that disposing of the action may as a practical matter impair or impede the movant's ability to protect its interest, unless existing parties adequately represent that interest." *Id.* at 1170-71 (quoting Fed. R. Civ. P. 24(a)(2)).[1]

Under Rule 24(b), the Court has discretion to permit a party to intervene in a case when that party "has a claim or defense that shares with the main action a common question of law or fact." Fed. R. Civ. P. 24(b)(1)(B). Courts undertake a two-step inquiry in determining whether permissive intervention under Rule 24(b) is proper. *Advance Loc. Media*, 918 F.3d at 1171. First, the intervenor must have "a claim or defense that shares with the main action a common question of law or fact," *Id.* (quoting Fed. R. Civ. P. 24(b)(1)(B)). Second, the court "must exercise discretion and consider whether the intervention will 'unduly delay or prejudice the adjudication of the original parties' rights.'" *Id.* (quoting Fed. R. Civ. P. 24(b)(3)); *accord Georgia Aquarium*, 309 F.R.D. at 690. And "[w]here intervention is sought only for a collateral purpose like unsealing documents, the ordinary requirements for permissive intervention are relaxed." *Vanda Pharms., Inc. v. Food & Drug Admin.*, No. CV 19-301 (JDB), 2021 WL 1820264, at *3 (D.D.C. May 6, 2021).

[1] To the extent this consideration is relevant in a case for limited intervention like this, there are plainly no parties to the litigation who can "adequately represent [FNN's] interest" in the sealed expert report because those parties are not currently subject to the litigation Dominion is pursuing against FNN. Fed. R. Civ. P. 24(a)(2).

### A. FNN has a claim or defense that shares common questions of fact with this litigation, sufficient for both intervention as of right and permissive intervention

FNN's "asserted interests for intervening—for the limited purpose of unsealing judicial records—provide[s] an adequate nexus for intervention." *Advance Loc. Media*, 918 F.3d at 1173 n.12 (analyzing Rule 24(b)). "Many circuits recognize that parties 'seeking to intervene in a case for the limited purpose of unsealing judicial records' need not show a 'strong nexus of fact or law' to the issues in the original case." *Id.* (quoting *Flynt v. Lombardi*, 782 F.3d 963, 967 (8th Cir. 2015); collecting other cases).[2]

Here, Plaintiffs' expert, Dr. Halderman, has produced a lengthy report detailing "numerous security vulnerabilities" in the Dominion voting system utilized

[2] *See also, e.g.*, *Jessup v. Luther*, 227 F.3d 993, 997-99 (7th Cir. 2000) ("[A]lthough there is ample justification for the common fact or law requirement when the proposed intervenors seek to become a party to the action, [t]here is no reason to require such a strong nexus of fact or law when a party seeks to intervene only for the purpose of modifying a protective order.") (internal quotation marks omitted); *Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 778 (3d Cir. 1994) ("By virtue of the fact that the Newspapers challenge the validity of the Order of Confidentiality entered in the main action, they meet the requirement of Fed. R. Civ. P. 24(b)(2) that their claim must have 'a question of law or fact in common' with the main action."); *In re Estelle*, 516 F.2d 480, 485 (5th Cir. 1975) ("The 'claim or defense' portion of the rule has been construed liberally, and indeed the Supreme Court has said that it 'plainly dispenses with any requirement that the intervenor shall have a direct personal or pecuniary interest in the subject of the litigation.'") (quoting *SEC v. U.S. Realty & Improvement Co.*, 310 U.S. 434, 459 (1940)).

in Georgia elections and warning that these “rather specific flaws in [Dominion’s] ICX software . . . can [be] exploit[ed] to steal votes on ICX devices.” Halderman Decl. ¶ 1; Halderman Rebuttal Decl. ¶ 2 (expressing similar concerns over the “numerous, critical vulnerabilities” that he had discovered during his review of the Dominion systems). Dr. Halderman further explains that his analysis indicates “that the ICX is very likely to contain other, equally critical flaws that are yet to be discovered.” Halderman Decl. ¶ 4. And Dr. Halderman notes the security problems are not limited to Georgia because the ICX systems are intended for use in parts of 16 states in the fast-approaching 2022 elections. *Id.*, ¶ 5, 8.

Whether Dominion’s voting systems suffer from serious security risks or are vulnerable to manipulation or voting fraud are factual questions that will play a prominent role in *Dominion v. FNN*. In that Delaware case, Dominion alleges that FNN defamed it by reporting on and repeating allegations raised by President Trump and his legal team that Dominion voting systems were used to commit election fraud in the 2020 presidential election. Although FNN contends that the falsity prong of the defamation inquiry should be limited to whether FNN accurately reported on the newsworthy allegations made by the president and his representatives, Dominion insists otherwise. Dominion insists that FNN can be held liable for defamation unless the underlying allegations made by the president’s representatives are true. Given this discrepancy—as well as the Delaware trial court's recent denial of FNN's motion to dismiss based, in part, on the need for further factual development of the issues—FNN has no choice but to investigate the veracity of allegations that Dominion's voting systems are not secure.

Publicly available documents filed in this Court demonstrate that Dr. Halderman's expert analysis for this case bears directly on this aspect of the *Dominion v. FNN* case. *See generally* Halderman Decl.; Halderman Rebuttal Decl. Moreover, these unsealed documents appear to only scratch the surface of Dr. Halderman's analysis: the sealed expert report is "a 25,000 word document that is the product of twelve weeks of intensive testing of the Dominion equipment provided" to Dr. Halderman for his examination that concludes that the Dominion system in use in Georgia "contains multiple severe security flaws." Halderman Rebuttal Decl. ¶ 4. So not only does the sealed report bear directly on FNN's litigation, the sealed report is not merely duplicative of any otherwise available documents. Consequently, providing access to FNN is the only way in which FNN could obtain the information contained in the expert report.

*Dominion v. FNN* relates to the factual questions covered in Dr. Halderman's sealed analysis for an additional reason: Dominion injected Dr. Halderman's expertise into its suit against FNN by alleging that Dr. Halderman "told [FNN] explicitly, 'There is absolutely no evidence, none, that Dominion Voting Machines changed any votes in this election.'" Compl. ¶ 68, *Dominion v. FNN*. FNN should thus be permitted to access Dr. Halderman's work in this litigation for the additional reason of determining, *inter alia*, whether his analysis here undermines his purported statement to FNN.[3]

### B. FNN has made a timely request that will not interfere with the pending litigation or prejudice any current parties, under both Rules 24(a) and 24(b)

All four factors governing timeliness weigh in FNN's favor:

> (1) the length of time during which the would-be intervenor knew or reasonably should have known of his interest in the case before petitioning for leave to intervene; (2) the extent of the prejudice that existing parties may suffer as a result of the would-be intervenor's failure to apply for intervention as soon as he actually knew or reasonably should have known of his interest; (3) the extent of the prejudice that the would-be intervenor may suffer if denied the opportunity to intervene; and (4) the existence of unusual circumstances weighing for or against a determination of timeliness.

*Advance Loc. Media*, 918 F.3d at 1171 (citation omitted). "The most important consideration in determining timeliness is whether any existing party to the litigation

[3] As demonstrated herein, FNN has a particularized interest in this specific expert report, which Louisiana did not have, making both FNN's right to obtain the report through intervention under Rule 24(a) and the case for permitting FNN to intervene under Rule 24(b) much stronger than any interest put forward by the State of Louisiana. And as FNN will demonstrate below, unlike Louisiana it does not readily have an alternative means of recreating Dr. Halderman's analysis, because FNN is not in possession of any state's Dominion election equipment and software.

will be harmed or prejudiced by the proposed intervenor's delay in moving to intervene." *Id.* (quoting *McDonald v. E. J. Lavino Co.*, 430 F.2d 1065, 1073 (5th Cir. 1970)).[4] Accordingly, the time between the commencement of the action and the motion to intervene is less important. *Id.* ("Intervention may be timely filed *even if* it occurs after a case has concluded") (emphasis added; collecting cases).

*First*, although this litigation has been pending since 2017, the expert report that is the subject of this intervention request was completed only six months ago, and it was only more recently than that when Dr. Halderman's declarations noting his significant concerns with Dominion's systems were publicly filed. Likewise, the trial court in Delaware denied FNN's motion to dismiss Dominion's case just a few weeks ago (on December 16, 2021). While that motion was pending, there remained the possibility that FNN would not need to seek Dr. Halderman's report, so FNN waited to involve this Court only when it became necessary for FNN to do so.

The few months between FNN learning of some of the contents of Dr. Halderman's sealed report and the filing of this motion is well within the multi-year periods the Eleventh Circuit and other courts have deemed acceptable. *E.g.*, *Advance Loc. Media*, 918 F.3d at 1171 n.9 ("[O]ther circuits have recognized that timeliness

[4] "[T]his [prejudice consideration] may well be *the only significant consideration* when the proposed intervenor seeks intervention of right." *Advance Loc. Media*, 918 F.3d at 1171 (emphasis added; quoting *McDonald*, 430 F.2d at 1073).

concerns may be less significant when intervention is ‘not on the merits, but for the sole purpose of challenging a protective order’”) (quoting *United Nuclear Corp. v. Cranford Ins. Co.*, 905 F.2d 1424, 1427 (10th Cir. 1990); collecting other cases).

*Second*, parties to the litigation will suffer no prejudice from FNN’s intervention. *Advance Loc. Media*, 918 F.3d at 1171. FNN does not seek to participate in the litigation beyond moving to unseal Dr. Halderman’s report for a limited purpose. In other words, FNN will not become a party to the litigation and this will not affect any other matters in this court—pending or forthcoming. The limited purpose for which FNN seeks intervention will ensure that there is no interference with the underlying litigation. There could thus be no possible prejudice to any of the parties in this litigation.

*Third*, denial of the motion to intervene would greatly prejudice FNN. It would impede FNN from obtaining a report from an expert who, following a thorough analysis of certain Dominion equipment and software, has determined that Dominion systems are plagued with “multiple severe security flaws,” Halderman Rebuttal Decl. ¶ 4, facts that are highly relevant to FNN’s defenses against Dominion’s claims. FNN has rights in accessing the information in the sealed report as a litigant in a case in which the contents of the report are highly relevant. *E.g.*, *Advance Loc. Media*, 918 F.3d at 1166, 1170. Denying FNN’s motion would frustrate FNN's "common law right to access the" report, and "[d]enial of this right constitutes an injury." *Id.* at 1172.

Dr. Halderman has made clear that he will not disclose his report to others while the report remains subject to the Court's protective order and AEO designation. Halderman Decl. ¶ 10 ("I of course have complied, and will continue to comply, with all directives from the Court regarding disclosure of my work in this matter."); *see also* Halderman Public Testimony Before the Louisiana Voting System Commission, Part 3, at 1:10:00 (Dec. 14, 2021), *available at* https://www.loom.com/share/d784b2995ead4cc69bf596bae3d1ce75 (explaining that this Court will determine whether Dr. Halderman's expert report will become publicly available).

Nor does FNN have as a "reasonable alternative[]" the ability to readily recreate Dr. Halderman's analysis, as the Court suggested that the Louisiana Secretary of State could do with its own Dominion machines. Doc. 1249 at 6. First, FNN does not possess any voting machines that were used in the 2020 elections (in Georgia, Louisiana, or elsewhere) so it cannot test machines it does not have. Second, while hiring "other similarly skilled election cyber engineering experts" to run similar tests to those run by Dr. Halderman might suffice for Louisiana to better protect the integrity of its future elections, *id.*, FNN has a particular interest in and need for Dr. Halderman's own analysis given the manner in which Dominion seeks to insert Dr. Halderman into the *Dominion v. FNN* case. So obtaining Dominion voting machines and retaining other experts would still not provide FNN the precise information—Dr. Halderman's analysis itself—which it has a right and a need to examine.

*Finally*, there are no "unusual circumstances weighing . . . against a determination of timeliness." *Id.* at 1171 (citation omitted).

Under the circumstances, FNN's motion is timely. *E.g.*, *Walker v. Jim Dandy Co.*, 747 F.2d 1360, 1365 (11th Cir. 1984) (articulating the following factors for the timeliness analysis: (1) the time period the intervenor should have known of its interest before seeking leave to intervene; (2) degree of prejudice to the existing parties due to the timing of the intervention; (3) prejudice to the intervenor if the request is denied; (4) any unusual circumstances militating either for or against a determination that the request is timely).

### C. The Court should exercise its discretion and grant FNN's request to intervene and grant FNN the requested limited access to Dr. Halderman's report

As demonstrated above, there is no impediment under Rule 24 to FNN's request to intervene in this litigation. The above considerations also demonstrate that the Court should grant the intervention request because to do so would not prejudice any party and to deny the intervention would prejudice FNN by impeding FNN from accessing an expert's analysis that is highly relevant to FNN's defense in separate litigation.[5]

Additionally, as explained below, FNN requests permission for a limited number of attorneys and consulting experts to view Dr. Halderman's expert report while the report retains its current level of confidentiality under the Court's protective order. Granting the motion to intervene for this limited purpose thus would not risk wide publication of the report while it retains a confidential designation in this litigation.

Finally, courts have long recognized that providing access to judicial documents helps to "secur[e] the integrity of the [judicial] process." *E.g.*, *Callahan v. United Network for Organ Sharing*, 17 F.4th 1356, 1361 (11th Cir. 2021) (explaining that this access is "an essential component of our system of justice" and

[5] FNN recognizes that the Court is considering the joint discovery request to allow some additional disclosure of Dr. Halderman's expert report. *See* Joint Disc. Statement Regarding Access to Pls.' Expert Report & Unduly Burdensome Disc., Doc. 1130 (July 12, 2021); *see also* Min. Entry, Doc. 1184 (Oct. 7, 2021). If the Court makes an unredacted version of the July 1, 2021 Halderman report available to the public, that could obviate the need for FNN's intervention. But the parties' request and the Court's minute order contemplate the Court making the expert report available on a more narrow basis that may not provide FNN sufficient access to the report, *id.*; *see also* Min. Entry, Doc. 1184 (Oct. 7, 2021), necessitating this motion to intervene at this time.

“instrumental in securing the integrity of the process. Providing FNN the limited access it seeks would serve to secure the integrity of the judicial process in the Delaware proceeding while maintaining the confidentiality required by the Court’s protective order.

## III. FNN Will Comply With the Confidentiality Measures Imposed By the Court’s Protective Order

FNN does not seek widespread dissemination of Dr. Halderman’s expert report. Rather, FNN seeks limited disclosure of the sensitive information contained in Dr. Halderman’s report for the reasons discussed above. FNN seeks access for 2 consulting experts and the following 4 counsel with Jackson Walker LLP, who represent FNN in *Dominion v. FNN*: Charles L. Babcock, Carl C. Butzer, John K. Edwards, and Joel Glover.

The persons accessing the report will abide by the confidentiality measures imposed by the Court in its protective order (Doc. 477). FNN will take steps to ensure that no other persons access the report by storing the confidential data in a manner accessible only to the named individuals.

## CONCLUSION

FNN respectfully requests that the Court grant its motion to intervene for the sole purpose of obtaining limited access to the expert report of Dr. J. Alex Halderman. A proposed order is attached hereto as Exhibit A.

Dated: January 12, 2022

*<u>/s/ Charles E. Peeler</u>*
Charles E. Peeler
Ga. Bar No. 570399
TROUTMAN PEPPER HAMILTON SANDERS LLP
Bank of America Plaza, Suite 3000
600 Peachtree Street N.E.
Atlanta, Georgia 30308-2216
Telephone: 404.885.3409
Email: charles.peeler@troutman.com

Charles L. Babcock
Application for Admission Pro Hac Vice pending
Joel Glover
Application for Admission Pro Hac Vice pending
JACKSON WALKER LLP
1401 McKinney Street, Suite 1900
Houston, TX 77010
Telephone: (713) 752-4210
Email: cbabcock@jw.com

Scott A. Keller
Application for Admission Pro Hac Vice pending
LEHOTSKY KELLER LLP
200 Massachusetts Avenue NW
Washington, DC 20001
Telephone: (512) 693-8350

*Attorney for Fox News Network, LLC*

**CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 5.1**

The undersigned hereby certifies that the foregoing document has been prepared in accordance with the font type and margin requirements of Local Rule 5.1 of the Northern District of Georgia, using a font type of Times New Roman and a point-size of 14.

*/s/ Charles E. Peeler*
Charles E. Peeler
Georgia Bar No. 570399
Troutman Pepper Hamilton Sanders LLP
Bank of America Plaza, Suite 3000
600 Peachtree Street N.E.
Atlanta, Georgia 30308-2216
Telephone: 404.885.3409
Email: Charles.peeler@troutman.com
*Attorney for Fox News Network, LLC*

## CERTIFICATE OF SERVICE

I hereby certify that on January 12, 2021, I electronically filed the forgoing Memorandum in Support of Motion to Intervene For Limited Purposes which will automatically send email notification of such filing to the attorneys of record.

*/s/ Charles E. Peeler*
Charles E. Peller
Georgia Bar No. 570399
Troutman Pepper Hamilton Sanders LLP
Bank of America Plaza, Suite 3000
600 Peachtree Street N.E.
Atlanta, Georgia 30308-2216
Telephone: 404.885.3409
Email: Charles.peeler@troutman.com
*Attorney for Fox News Network, LLC*