PARKER DANIELS KIBORT
Andrew Parker (028314)
888 Colwell Building
123 Third Street North
Minneapolis, Minnesota 55401
Telephone: (612) 355-4100
Facsimile: (612) 355-4101
Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Kari Lake and Mark Finchem,

Plaintiffs,

v.

Kathleen Hobbs, as Arizona Secretary of State; Bill Gates, Clint Hickman, Jack Sellers, Thomas Galvin, and Steve Gallardo, in their capacity as members of the Maricopa County Board of Supervisors; Rex Scott, Matt Heinz, Sharon Bronson, Steve Christy, Adelita Grijalva, in their capacity as members of the Pima County Board of Supervisors,

Defendants.

No. _____

COMPLAINT

(Jury Trial Demanded)

1. This is a civil rights action for declaratory and injunctive relief to prohibit the use of electronic voting machines in the State of Arizona in the upcoming 2022 Midterm Election, slated to be held on November 8, 2022 (the "Midterm Election"), unless and until the electronic voting system is made open to the public and subjected to scientific analysis by objective experts to determine whether it is secure from manipulation or intrusion. The machine companies have consistently refused to do this.

2. Plaintiffs have a constitutional and statutory right to have their ballots, and all ballots cast together with theirs, counted accurately and transparently, so that only legal votes determine the winners of each office contested in the Midterm Election. Electronic voting machines cannot be deemed reliably secure and do not meet the constitutional and statutory mandates to guarantee a free and fair election. The use of untested and unverified electronic voting machines violates the rights of Plaintiffs and their fellow voters and office seekers, and it undermines public confidence in the validity of election results. Just as the government cannot insist on "trust me," so too, private companies that perform governmental functions, such as vote counting, cannot be trusted without verification

3. Defendants each have duties to ensure elections held with a "maximum degree of correctness, impartiality, uniformity and efficiency on the procedures for early voting and voting, and of producing, distributing, collecting, counting, tabulating and storing ballots." A.R.S. § 16-452 (A). Defendants have fallen short of those duties, and they will do so again unless this Court intervenes.

4. For two decades, experts and policymakers from across the political spectrum have raised glaring failures with electronic voting systems. Indeed, just three months ago, a computer science expert in *Curling v. Raffensperger*, Case No. 1:17-cv-02989-AT (U.S. Dist. Ct., N.D. Ga.), identified catastrophic failures in electronic voting machines used in sixteen states, including Arizona. The expert testified that the failures include the ability to defeat all state safety procedures. This caused the Cybersecurity and Infrastructure Security Agency ("CISA") to enter an appearance and urge the federal district court to not allow disclosure of the

expert's report detailing these failures. The district court refused to allow disclosure of that expert report to date. Secrecy destroys public confidence in our elections and election systems that result in secrecy undermine our democratic process.

5. The problems with the electronic voting systems are not only technical, but structural. To date, only three companies collectively provide voting machines and software for 90% of all eligible voters in the United States. Most of those machines are over a decade old, have critical components manufactured overseas in countries, some of which are hostile to the United States, and use software that is woefully outdated and vulnerable to catastrophic cyberattacks. Indeed, countries like France have banned the use of electronic voting machines due to lack of security and related vulnerabilities.

6. Given the limitations and flaws of existing technology, electronic voting machines cannot legally be used to administer elections today and for the foreseeable future, unless and until their current electronic voting system is objectively validated.

7. Through this Action, Plaintiffs seek an Order that Defendants collect and count votes through a constitutionally acceptable process, which relies on tried and true precepts that mandates integrity and transparency. This includes votes cast by hand on verifiable paper ballots that maintains voter anonymity; votes counted by human beings, not by machines; and votes counted with transparency, and in a fashion observable to the public.

8. It is important to note that this Complaint is not an attempt to undo the past. Most specifically, it is not about undoing the 2020 presidential election. It is only about the future – about upcoming elections that will employ voting machines designed and run by private

companies, performing a crucial governmental function, that refuse to disclose their software and system components and subject them to neutral expert evaluation. It raises the profound constitutional issue: can government avoid its obligation of democratic transparency and accountability by delegating a critical governmental function to private companies?

I. INTRODUCTION

9. Defendant Hobbs, as Arizona Secretary of State and the chief election officer in Arizona, has violated state and federal law. Defendant Hobbs' violations include failing to:

- Achieve and maintain the maximum degree of correctness, impartiality, uniformity in elections.
- Ensure that all votes are counted safely, efficiently, and accurately.
- Ensure that all software code, firmware code, and hard-coded instructions on any hardware component used, temporarily or installed in the voting systems, precludes fraud or any unlawful act.
- Revoke the certification of electronic voting systems used in elections in Arizona.
- Demand access to the electronic voting system so that it can be examined by objective experts.

10. Defendant Hobbs intends to commit these same violations up to and during the Midterm Election.

11. Defendants Gates, Hickman, Sellers, Galvin, and Gallardo, as Members of the Maricopa County Board of Supervisors, have caused the use of election systems and equipment in Maricopa County that are rife with potentially glaring cybersecurity vulnerabilities, including

- Operating systems lacking necessary updates;
- Antivirus software lacking necessary updates;
- Open ports on the election management server, allowing for possible remote access;

- Shared user accounts and common passwords;
- Anomalous, anonymous logins to the election management server;
- Unexplained creation, modification, and deletion of election files;
- Lost security log data;
- The presence of stored data from outside of Maricopa County;
- Unmonitored network communications;
- Unauthorized user internet or cellular access through election servers and devices.
- Secret content not subject to objective and public analysis.

12. Pima County uses election equipment and systems that are in substance and defect the same as the equipment and systems used in Maricopa County. Defendants Scott, Heinz, Bronson, Christy, and Grijalvaas, as Members of the Pima County Board of Supervisors, have caused the use of election systems and equipment in Pima County that are rife with the same glaring potential cybersecurity vulnerabilities present in the Maricopa County equipment.

13. Every county in Arizona intends to tabulate votes cast in the Midterm Elections through optical scanners, the vast majority of which are manufactured by Election Systems & Software ("ES&S") or Dominion Voting Systems ("Dominion").

14. After votes are tabulated at the county level using these machines through these companies' proprietary election management systems, the vote tallies will be uploaded over the internet to an election reporting system.

15. Some voters in Arizona will rely on electronic voting systems to cast their votes as well as tabulate them. Voters who may have hearing or visual impairments may cast their votes

with the aid of electronic ballot marking devices manufactured primarily by ES&S or Dominion. These voters' electoral choices are even more vulnerable to attack and manipulation, as ballot marking devices pose significant security risks on their own.

16. Defendant Hobbs, through the website of the Office of the Arizona Secretary of State, has represented that counties throughout Arizona will rely on electronic voting systems in the Midterm Election.

17. Defendant Hobbs on or about November 5, 2019, certified the Dominion Democracy Suite 5.5b voting system for use in elections held in Arizona. This voting system, as well as the component parts identified above, will be used in the Midterm Election.

18. Defendant Hobbs after July 22, 2020, certified the ES&S ElectionWare 6.0.40 voting system, as well as its component parts, for use in elections held in Arizona. This voting system, as well as the component parts identified above, will be used in the Midterm Election.[1]

19. Defendant Hobbs's certification of the Dominion Democracy Suite 5.5b voting system, as well as its component parts, was improper, absent objective evaluation.

20. Defendant Hobbs's certification of the ES&S ElectionWare 6.0.40 voting system, as well as its component parts, was improper.

21. Defendant Hobbs has the authority to revoke the certification of every voting system, including all component parts thereto, certified by the State of Arizona. Defendant Hobbs has improperly failed to exercise that authority.

[1] See https://azsos.gov/elections/voting-election/voting-equipment.

22. All optical scanners and ballot marking devices certified by Arizona, as well as the software on which they rely, have been wrongly certified for use in Arizona. These systems are potentially unsecure, lack adequate audit capacity, fail to meet minimum statutory requirements, and deprive voters of the right to have their votes counted and reported in an accurate, auditable, legal, and transparent process. Using them in the upcoming elections, without objective validation, violates the voting rights of every Arizonan.

23. All electronic voting machines and election management systems, including those slated to be used in Arizona in the Midterm Election, can be manipulated through internal or external intrusion to alter votes and vote tallies.

24. Specific vulnerabilities in the electronic voting machines used by Maricopa County have been explicitly identified and publicized in analyses by cybersecurity experts, even absent access to the systems.

25. Substantially similar vulnerabilities in electronic voting machines in general have been identified and publicized in analyses presented to various congressional committees. All electronic voting machines can be connected to the internet or cellular networks, directly or indirectly, at various steps in the voting, counting, tabulating, and/or reporting process.

26. Voting machines and systems used in Arizona contain electronic components manufactured or assembled in foreign nations which have attempted to manipulate the results of U.S. elections.

27. Electronic voting machines and software manufactured by industry leaders, specifically including Dominion and ES&S, are vulnerable to cyberattacks before, during, and after an election in a manner that could alter election outcomes.

28. These systems can be connected to the internet or cellular networks, which provides an access point for unauthorized manipulation of their software and data. They often rely on outdated versions of Windows, which lack necessary security updates. Both of these common shortcomings leave the systems vulnerable to generalized, widespread-effect attacks.

29. Since 2000, alleged, attempted, and actual illegal manipulation of votes through electronic voting machines has apparently occurred on multiple occasions.

30. Expert testimony demonstrates that all safety measures intended to secure electronic voting machines against manipulation of votes, such as risk limiting audits and logic and accuracy tests, can be defeated.

31. Other countries, including France and Taiwan, have completely or largely banned or limited the use of electronic voting machines due to the security risks they present.

32. Arizona's electronic election infrastructure is potentially susceptible to malicious manipulation that can cause incorrect counting of votes. Despite a nationwide bipartisan consensus on this risk, election officials in Arizona continue to administer elections dependent upon unreliable, insecure electronic voting systems. These officials, including Defendants in Maricopa County, refuse to take necessary action to address known and currently unknown election security vulnerabilities, and in some cases have obstructed court authorized inspections of their electronic voting systems.

33. Plaintiffs seek the intervention of this Court because the Secretary of State and county officials throughout the State have failed to take constitutionally necessary measures to protect voters' rights to a secure and accurately counted election process. The State of Arizona and its officials bear a legal, constitutional, and ethical obligation to secure the State's electoral system, but they lack the will to do so.

I. PARTIES

34. Plaintiff Kari Lake is a candidate for Governor of Arizona, an office she seeks in the Midterm Election.

35. Plaintiff Kari Lake is also a resident of the State of Arizona, registered to vote in Maricopa County, who intends to vote in Arizona in the Midterm Election.

36. Plaintiff Mark Finchem is a sitting member of the Arizona House of Representatives and a candidate for Secretary of State of Arizona, an office he seeks in the Midterm Election.

37. Plaintiff Mark Finchem is also a resident of the State of Arizona, registered to vote in Pima County, who intends to vote in Arizona in the Midterm Election.

38. Plaintiff Lake has standing to bring this action as an intended voter in the Midterm Election and as a "qualified elector" under A.R.S. § 16-121. As a candidate for Governor of Arizona Plaintiff Lake further has standing as an aggrieved person to bring this action.

39. Plaintiff Finchem, in his capacity as a member of the Arizona House of Representatives charged with upholding the Constitution of the United States, has standing to bring this action.

40. Plaintiff Finchem has standing to bring this action as an intended voter in the Midterm Election and as a "qualified elector" under A.R.S. § 16-121. As a candidate for Secretary of State of Arizona Plaintiff Finchem further has standing as an aggrieved person to bring this action.

41. Defendant Hobbs is, through this Complaint, sued for prospective declaratory and injunctive relief in her official capacity as the Secretary of State of Arizona, together with any successor in office automatically substituted for Defendant Hobbs by operation of Fed. R. Civ. P. 25(d).

42. In her official capacity, Defendant Hobbs is the chief election officer for the State of Arizona. Defendant Hobbs is responsible for the orderly and accurate administration of public election processes in the state of Arizona. This responsibility includes a statutory duty to ensure that "satisfactorily tested" voting systems are used to administer public elections, A.R.S. § 16-441, and to conduct any reexaminations of previously adopted voting systems, upon request or at Defendant Hobbs's own discretion.

43. Defendant Hobbs is further required by law to determine the voting equipment that is to be used to cast and count the votes in all county, state, and federal elections in Arizona. A.R.S. §§ 16-446, 16-452.

44. Defendants Bill Gates, Clint Hickman, Jack Sellers, Thomas Galvin, and Steve Gallardo (collectively "Maricopa Defendants") are sued for prospective declaratory and injunctive relief in their official capacities as members of the Maricopa County Board of Supervisors ("Maricopa Board").

45. Defendants Scott, Heinz, Bronson, Christy, and Grijalva (collectively "Pima Defendants") are sued for prospective declaratory and injunctive relief in their official capacities as members of the Pima County Board of Supervisors ("Pima Board").

46. Under A.R.S. § 16-452 (A), the Maricopa Board and the Pima Board are vested with the authority to:

- "[e]stablish, abolish and change election precincts, appoint inspectors and judges of elections, canvass election returns, declare the result and issue certificates thereof…";
- "[a]dopt provisions necessary to preserve the health of the county, and provide for the expenses thereof";
- "[m]ake and enforce necessary rules and regulations for the government of its body, the preservation of order and the transaction of business."

II. JURISDICTION AND VENUE

47. Plaintiffs bring this action under 42 U.S.C. § 1983 and the cause of action recognized in *Ex parte Young*, 209 U.S. 123 (1908), and its progeny to challenge government officers' "ongoing violation of federal law and [to] seek[] prospective relief" under the equity jurisdiction conferred on federal district courts by the Judiciary Act of 1789.

48. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1343 because this action seeks to protect civil rights under the Fourteenth Amendment to the United States Constitution.

49. This Court has supplemental jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1367.

50. This Court has authority to grant declaratory relief based on 28 U.S.C. §§ 2201 & 2202, and Rule 57 of the Federal Rules of Civil Procedure.

51. This Court has jurisdiction to grant injunctive relief based on 28 U.S.C. § 1343(a)(3) and authority to do so under Federal Rule of Civil Procedure 65.

52. This Court has jurisdiction to award nominal and compensatory damages under 28 U.S.C. § 1343(a)(4).

53. This Court has authority to award reasonable attorneys' fees and costs. 28 U.S.C. § 1920 and 42 U.S.C. § 1988(b).

54. Venue is proper in this Court under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

55. This Court has personal jurisdiction over all Defendants because all defendants reside and are domiciled in the State of Arizona. Requiring Defendants to litigate these claims in the United States District Court for the District of Arizona does not offend traditional notions of fair play and substantial justice and is permitted by the Due Process Clause of the United States Constitution.

III. FACTUAL ALLEGATIONS

A. Background

56. Arizona intends to rely on electronic voting systems to record some votes and to tabulate *all* votes cast in the State of Arizona in the 2022 Midterm Election, without disclosing the systems and subjecting them to neutral, expert analysis.[2]

[2] https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2022/state/4

57. Prior to 2002, most states, including Arizona, conducted their elections overwhelmingly using relatively secure, reliable, and auditable paper-based systems.

58. After the recount of the 2000 presidential election in Florida and the ensuing *Bush v. Gore* decision, Congress passed the Help America Vote Act in 2002.[3] In so doing, Congress opened the proverbial spigot. Billions of federal dollars were spent to move states, including Arizona, from paper-based voting systems to electronic, computer-based systems.

59. Since 2002, elections throughout the United States have increasingly and largely been conducted using a handful of computer-based election management systems. These systems are created, maintained, and administered by a small number of companies having little to no transparency to the public, producing results that are far more difficult to audit than paper-based systems, and lack any meaningful federal standards or security requirements beyond what individual states may choose to certify. Leaders of both major parties have expressed concern about this lack of transparency, analysis and accountability.

60. As of 2019, Dominion, ES&S, and one other company (Hart InterCivic) supplied more than ninety percent of the nationwide "voting machine market."[4] Dominion and ES&S control even more than that share of the market in Arizona. All three of these providers' electronic voting machines can be hacked or compromised with malware, as has been demonstrated by recognized computer science experts, including experts from the University of

[3] 52 U.S.C. § 20901 *et seq*.

[4] Pam Fessler & Johnny Kauffman, *Trips to Vegas and Chocolate-Covered Pretzels: Election Vendors Come Under Scrutiny*, NPR (May 2, 2019) (https://www.npr.org/2019/05/02/718270183/trips-to-vegas-and-chocolate-covered-pretzels-election-vendors-come-under-scruti).

Michigan, Princeton University, Georgetown University, and other institutions and presented to various congressional committees. All can be, and at various steps in the voting, counting, tabulating, and/or reporting process are designed to be, connected to the internet or cellar networks, directly or indirectly.

61. This small cadre of companies supplies the hardware and software for the electronic voting machines, in some cases manages the voter registration rolls, maintains the voter records, partially manages the elections, programs the vote counting, and reports the election results.

62. Jurisdictions throughout the nation, including Arizona, have functionally outsourced all election operations to these private companies. In the upcoming Midterm Election, over three thousand counties across the United States will have delegated the governmental responsibility for programming and administering elections to private contractors.

63. This includes all counties in Arizona, most of which have contracted with Dominion or ES&S to provide machines, software, and services for the Midterm Election. For example, in Defendant Maricopa County, officials do not possess credentials necessary to validate tabulator configurations and independently validate the voting system prior to an election. Dominion maintains those credentials.

64. By its own account, Dominion provides an "End-To-End Election Management System" that "[d]rives the entire election project through a single comprehensive database."[5] Its

[5] DEMOCRACY SUITE® ELECTION MANAGEMENT SYSTEM, https://www.dominionvoting.com/democracy-suite-ems/ (last visited Apr. 22, 2022).

tools "build the election project," and its technology provides "solutions" for "voting & tabulation," and "tallying & reporting," and "auditing the election." The products sold by Dominion include ballot marking machines, tabulation machines, and central tabulation machines, among others.

65. Dominion, in its normal course of business, including the Midterm Election in Arizona, manufactures, distributes, and maintains voting hardware and software. Dominion also executes software updates, fixes, and patches for its voting machines and election management systems.

66. After votes are tabulated at the county level using Dominion's electronic election management system in the Midterm Election, the vote tallies will be uploaded over the internet to an election reporting system.

67. Dominion's machines and systems range from the "election event designer"—software that creates the ballots voters will mark while voting, as well as programing the tabulators of those votes—to the devices on which voters mark their votes ("ballot marking devices," or "BMDs"), to the machines that tabulate the votes at the precinct level, to the machines that receive and tabulate the various precinct results ("centralized tabulation"), to the systems and options for transmitting those results from the BMD to the precinct tabulator to the central tabulator to, ultimately, the official government authority responsible for certifying the election results. In the Midterm Election, many Arizonans will cast their votes on Dominion BMDs, while nearly *all* Arizonans will have their votes tabulated with Dominion machines.

68. Dominion controls the administration and conduct of the elections in those jurisdictions where its systems are deployed, including Arizona. Any vulnerabilities or weaknesses in Dominion's systems, at the very least, call into question the integrity and reliability of all election results coming from those jurisdictions. Dominion has refused to disclose its software and other parts of its electronic voting systemin order to subject it to neutral expert evaluation.

69. As an example, following the 2020 election an audit of election processes and results in Maricopa County, Arizona was ordered. It was concluded that:

- "The official result totals do not match the equivalent totals from the Final Voted File (VM55). These discrepancies are significant with a total ballot delta of 11,592 between the official canvass and the VM55 file when considering both the counted and uncounted ballots.";

- "…a large number of files on the Election Management System (EMS) Server and HiPro Scanner machines were deleted including ballot images, election related databases, result files, and log files. These files would have aided in our review and analysis of the election systems as part of the audit. The deletion of these files significantly slowed down much of the analysis of these machines. Neither of the 'auditors' retained by Maricopa County identified this finding in their reports."; and

- "Despite the presence of at least one poll worker laptop at each voting center, the auditors did not receive laptops or forensic copies of their hard drives. It is unknown, due to the lack of this production, whether there was unauthorized access, malware present or internet access to these systems."

B. Decades of Evidence Prove Electronic Voting Systems Do Not Provide a Secure, Transparent, or Reliable Vote

70. Over the last two decades the United States has transitioned from a safe, secure, auditable paper-based system to an inherently vulnerable, network-exposed electronic equipment-based system. The transition to increased reliance on electronic systems and

computer technology has created unjustified new risks of hacking, election tampering, and electronic voting fraud.

71. With each passing election the unreliability of electronic voting machines has become more apparent. In light of this experience, the vote tallies reported by electronic voting machines cannot, without objective evaluation, be trusted to accurately show which candidates actually received the most votes.

72. Credible allegations of electronic voting machine "glitches" that materially impacted specific races began to emerge in 2002. *Black Box Voting,* the seminal publication documenting early pitfalls of electronic voting systems, chronicles the following failures:

> In the Alabama 2002 general election, machines made by Election Systems and Software (ES&S) flipped the governor's race. Six thousand three hundred Baldwin County electronic votes mysteriously disappeared after the polls had closed and everyone had gone home. Democrat Don Siegelman's victory was handed to Republican Bob Riley, and the recount Siegelman requested was denied. Six months after the election, the vendor shrugged. "Something happened. I don't have enough intelligence to say exactly what," said Mark Kelley of ES&S.
>
> […]
>
> In the 2002 general election, a computer miscount overturned the House District 11 result in Wayne County, North Carolina. Incorrect programming caused machines to skip several thousand partyline votes, both Republican and Democratic. Fixing the error turned up 5,500 more votes and reversed the election for state representative.
>
> […]
>
> Voting machines failed to tally "yes" votes on the 2002 school bond issue in Gretna, Nebraska. This error gave the false impression that the measure had failed miserably, but it actually passed by a 2 to 1 margin. Responsibility for the errors was attributed to ES&S, the Omaha company that had provided the ballots and the machines.
>
> […]
>
> In the November 2002 general election in Scurry County, Texas, poll workers got suspicious about a landslide victory for two Republican commissioner candidates. Told that a "bad chip" was to blame, they had a new computer chip flown in and also counted

the votes by hand — and found out that Democrats actually had won by wide margins, overturning the election.[6]

73. By 2004, explicit evidence that electronic voting machines were susceptible to intentional manipulation, and that malicious actors sought to exploit this vulnerability, became public. In that year, cyber expert Clint Curtis testified under oath before the House Judiciary Committee that he had previously been hired to create a program that would change the results of an election without leaving any trace of the change. He claimed he wrote this program with ease. Mr. Curtis' testimony can be watched here: https://www.youtube.com/watch?v=JEzY2tnwExs.

74. During the next election cycle, in 2006, a team of computer scientists at Princeton University analyzed the Diebold AccuVote-TS voting machine, then one of the most widely-deployed electronic voting platforms in the United States. They found, "Malicious software running on a single voting machine can steal votes with little risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss. . . . Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute. . . . AccuVote-TS machines are susceptible to voting machine viruses – computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre- and post-election activity." The Princeton team prepared a video demonstration showing how malware could flip votes. In the video, mock election votes were

[6] Available at https://blackboxvoting.org/black-box-voting-book/.

cast in favor of George Washington by a 4 to 1 margin, but the paper print-out that reported the results showed Benedict Arnold prevailing by a margin of 3 to 2. Malicious vote-stealing malware was the sole reason for reallocation of votes. The malware deleted itself after the election, leaving no evidence that the voting machine was ever hijacked or any votes stolen.

75. In 2009 Diebold sold (at a loss) "Premier," its electronic voting systems business unit, which by then was known for its technical problems and unreliable security and accuracy. The Premier intellectual property passed (from ES&S) to Dominion in May 2010. That intellectual property included the GEMS election management system software. Dominion quickly incorporated GEMS into its own products and by 2011 was selling election equipment that had updated GEMS software at its heart. But GEMS was notorious for being, according to Harper's Magazine, "a vote rigger's dream" that "could be hacked, remotely or on-site, using any off-the-shelf version of Microsoft Access, and password protection was missing for supervisor function." Lack of encryption on its audit logs "allowed any trace of vote rigging to be wiped from the record." Computer scientists from Johns Hopkins University and Rice University found GEMS "far below even the most minimal security standards applicable in other contexts" and "unsuitable for use in a general election."

76. In 2015 the Brennan Center for Justice issued a report listing two and a half-pages of instances of issues with voting machines, including a 2014 investigation which found "voters in Virginia Beach observed that when they selected one candidate, the machine would register

their selection for a different candidate."[7] The investigation also found that the Advanced Voting Solutions WINVote machine, which is Wi-Fi-enabled, "had serious security vulnerabilities" because wireless cards on the system could allow "an external party to access the [machine] and modify the data [on the machine] without notice from a nearby location," and "an attacker could join the wireless ad-hoc network, record voting data or inject malicious [data.]"

77. In 2016, following in the footsteps of the Johns Hopkins, Rice, and 2006 Princeton teams, Princeton Professor of Computer Science Andrew Appel told an interviewer how he had purchased a voting machine for $82 on the internet – the Sequoia AVC Advantage, still set to be used in the 2016 election in a number of states – and replaced the machine's ROM chips in mere minutes using little more than a screwdriver, thereby "throw[ing] off the machine's results, subtly altering the tally of votes, never to betray a hint to the voter."[8]

[7] Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, p.13 (Sep. 15, 2014) (available at https://www.brennancenter.org/our-work/research-reports/americas-voting-machines-risk).

[8] Ben Wofford, *How to Hack an Election in 7 Minutes,* Politico (Aug. 5, 2016) (https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144/).

78. During that 2016 election cycle evidence emerged of foreign state actors seeking to affect U.S. voting. "Russian agents probed voting systems in all 50 states, and successfully breached the voter registration systems of Arizona and Illinois."[9] The Robert Mueller report and an indictment of twelve Russian agents later confirmed that Russian hackers had targeted vendors that provide election software, and Russian intelligence officers "targeted employees of [REDACTED], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network."[10]

79. After these revelations about the 2016 election, Jake Braun, a former security advisor for the Obama administration and organizer of the DEFCON Hacking Conference was

---

[9] Jordan Wilkie, *'They think they are above the law': the firms that own America's voting system*, The Guardian (Apr. 23, 2019) (https://www.theguardian.com/us-news/2019/apr/22/us-voting-machine-private-companies-voter-registration).

[10] Robert S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, vol. 1, p. 51 (Mar. 2019). (https://www.justice.gov/archives/sco/file/1373816/download).

asked in 2017, "Do you believe that right now, we are in a position where the 2020 election will be hacked?" He answered, "Oh, without question. I mean the 2020 election will be hacked no matter what we do."

80. Following a 2017 runoff election in a Georgia congressional race, an advocacy organization and individual voters filed suit in federal district court seeking to set aside the results. They alleged the election "took place in an environment in which sophisticated hackers – whether Russian or otherwise – had the capability and intent to manipulate elections in the United States" and had "easy access" to do so.

81. The Georgia plaintiffs supported their allegations with expert testimony from Logan Lamb, who testified that he freely accessed official Georgia state election files hosted on an "elections.kennesaw.edu" server, including voter histories and personal information of all Georgia voters; tabulation and memory card programming databases for past and future elections; instructions and passwords for voting equipment administration; and executable programs controlling essential election resources. Lamb stated that these sensitive files had been publicly exposed for so long that Google had cached (i.e., saved digital backup copies of) and published the pages containing many of them. Lamb said the publicly accessible files created and maintained on this server were used to program virtually all other voting and tabulation equipment used in Georgia's elections.

82. Another piece of expert evidence in the Georgia litigation is a declaration from Harri Hurst dated August 24, 2020 in which Hursti concludes that "the voting system is being operated in Fulton County in a manner that escalates the security risk to an extreme level."

Hursti based this conclusion in part on his observations that optical scanners would inexplicably reject ballots; that the optical scanners would experience lengthy and unexplained scanning delays; that the vendor, Dominion, failed to ensure a trained technician was on-site to address problems with its equipment; that Dominion employees interfered with Hursti's efforts to observe the upload of memory devices; that Dominion refused to cooperate with county personnel; and that computers running Dominion software were vulnerable due to inadequate "hardening" against a security attack.[11]

83. The Georgia plaintiffs asked the court to enter a preliminary injunction barring Georgia in the 2020 general election from using certain Dominion electronic voting machines. On October 11, 2020, the federal court issued an order finding substantial evidence that the system was plagued by security risks and the potential for votes to be improperly rejected or misallocated. It wrote, "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.'"

84. In 2019 a group of election security experts found "nearly three dozen backend election systems in 10 states connected to the internet over the last year," including in "critical swing states" Wisconsin, Michigan, and Florida. Some of the jurisdictions "were not aware that their systems were online" and were "publicly saying that their systems were never connected to

[11] *Curling v. Raffensperger*, Case No. 1:17-cv-02989-AT (U.S. Dist. Ct., N.D. Ga.), ECF Doc. 809-3.

the internet because they didn't know differently."[12] The Associated Press reported that the vast majority of 10,000 election jurisdictions nationwide were still using Windows 7 or older operating systems to create ballots, program voting machines, tally votes, and report counts, which was a problem because "Windows 7 reaches its 'end of life' on Jan. 14 [2020], meaning Microsoft stops providing technical support and producing "patches" to fix software vulnerabilities, which hackers can exploit."[13]

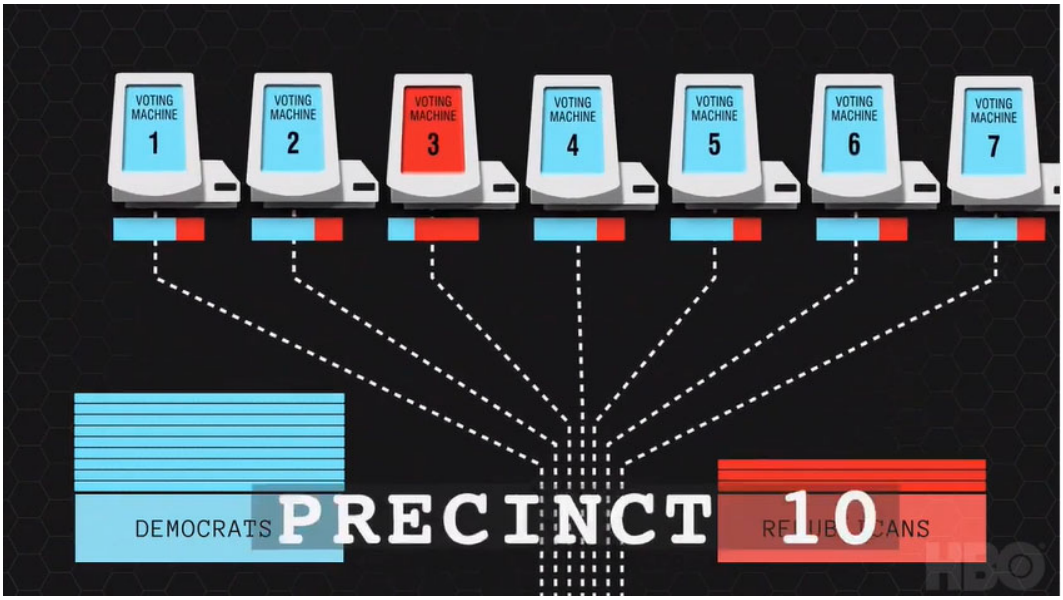
85. In March 2020, the documentary *Kill Chain: The Cyber War on America's Elections* detailed the vulnerability of electronic voting machines. In the film, Hursti showed that he hacked digital election equipment to change votes back in 2005, and said the same Dominion machine that he hacked in 2005 was slated for use in 20 states for the 2020 election. *Kill Chain* also included facts about a Georgia election in which one machine out of seven in a precinct registered a heavy majority of Republican votes, while every other machine in the precinct registered a heavy majority of Democratic votes. Dr. Kellie Ottoboni, Department of Statistics, UC Berkeley, stated the likelihood of this happening by chance was less than one in a million.[14]

---

[12] Kim Zetter, *Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials*, Vice (Aug. 8, 2019) (https://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials).

[13] Tami Abdollah, *New election systems use vulnerable software*, Associated Press (July 13, 2019) (https://apnews.com/article/operating-systems-ap-top-news-voting-voting-machines-pennsylvania-e5e070c31f3c497fa9e6875f426ccde1).

[14] Screenshot from https://www.facebook.com/KillChainDoc/videos/2715244992032273/.



C. Electronic Voting Systems Manufacturers Source and Assemble Their Components in Hostile Nations

86. Electronic voting machines are also vulnerable to malicious manipulation through illicit software installed on their component parts during the manufacturing process. The Congressional Task Force on Election Security's Final Report in January 2018 stated, "many jurisdictions are using voting machines that are highly vulnerable to an outside attack," in part because "many machines have foreign-made internal parts." Therefore, "'[A] hacker's point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line.'"[15]

87. Computer server security breaches as a result of hardware manufactured in China have been discovered by the U.S. Department of Defense (2010), Intel Corp. (2014), an FBI

[15] CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT at 25 (2018) (https://homeland.house.gov/imo/media/doc/TFESReport.pdf).

investigation that affected multiple companies (2015), and a government contractor providing intelligence services (2018).[16]

88. Leading electronic voting machine manufacturers source many parts from China, Taiwan, and the Philippines.[17]

D. State and Federal Lawmakers from Both Parties Have Long Been Aware of the Problems with Electronic Voting Systems

89. As the years passed and the evidence mounted, lawmakers and officials throughout the nation have realized these problems with electronic voting machines cannot be ignored.

90. The Congressional Task Force on Election Security issued a Final Report in January 2018 that identified the vulnerability of U.S. elections to foreign interference:[18] "According to DHS, Russian agents targeted election systems in at least 21 states, stealing personal voter records and positioning themselves to carry out future attacks. . . media also reported that the Russians accessed at least one U.S. voting software supplier . . . in most of the targeted states officials saw only preparations for hacking . . . [but] in Arizona and Illinois, voter registration databases were reportedly breached. . . If 2016 was all about preparation, what more

---

[16] Jordan Robertson and Michael Riley, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, Bloomberg (October 4, 2018). (https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies).

[17] Ben Popken, Cynthia McFadden and Kevin Monahan, *Chinese parts, hidden ownership, growing scrutiny: Inside America's biggest maker of voting machines*, NBC News (Dec. 19, 2019) (https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-inside-america-s-biggest-n1104516).

[18] CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT (2018) (https://homeland.house.gov/imo/media/doc/TFESReport.pdf).

can they do and when will they strike? . . . [W]hen asked in March about the prospects for future interference by Russia, then-FBI Director James Comey testified before Congress that: '[T]hey'll be back. They'll be back in 2020. They may be back in 2018.'"[19]

91. In a March 21, 2018 hearing held by the Senate Intelligence Committee relating to potential foreign interference in the 2016 election, Senator Ron Wyden warned that:

> Forty-three percent of American voters use voting machines that researchers have found have serious security flaws including backdoors. These companies are accountable to no one. They won't answer basic questions about their cyber security practices and the biggest companies won't answer any questions at all. Five states have no paper trail and that means there is no way to prove the numbers the voting machines put out are legitimate. So much for cyber-security 101… The biggest seller of voting machines is doing something that violates cyber-security 101, directing that you install remote-access software which would make a machine like that a magnet for fraudsters and hackers.

92. Senator Wyden did not see his concerns addressed. On December 6, 2019, he, along with his Democratic colleagues in Congress – Senator Elizabeth Warren, Senator Amy Klobuchar, and Congressman Mark Pocan – published an open letter concerning major voting system manufacturers. In the letter, they identified numerous problems:

- "trouble-plagued companies" responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems."

- "the election technology industry has become highly concentrated ... Today, three large vendors – Election Systems & Software, Dominion, and Hart InterCivic – collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States."

- "Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. . . . voting machines are reportedly

[19] *Id*. at 6-7.

falling apart, across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk. . . . Moreover, even when state and local officials work on replacing antiquated machines, many continue to 'run on old software that will soon be outdated and more vulnerable to hackers.'"

- "[J]urisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems-leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.[]"

93. Senator Warren, on her website, identified an additional problem: "These vendors make little to no information publicly available on how much money they dedicate to research and development, or to maintenance of their voting systems and technology. They also share little or no information regarding annual profits or executive compensation for their owners."

94. During a Senate Judiciary Committee hearing in June 2018, then-Senator Kamala Harris warned that, in a demonstration for lawmakers at the Capitol, election machines were "hacked" before the lawmakers' eyes. Two months later, Senator Klobuchar stated on national television, "I'm very concerned you could have a hack that finally went through. You have 21 states that were hacked into, they didn't find out about it for a year."

95. While chairing the House Committee on Homeland Security in July of 2018, Republican Congressman Michael McCaul decried, "Our democratic system and critical infrastructures are under attack. In 2016, Russia meddled in our Presidential election through a series of cyber attacks and information warfare. Their goals were to undermine the credibility of the outcome and sow discord and chaos among the American people…."

96. Senator Wyden stated in an interview, "[T]oday, you can have a voting machine with an open connection to the internet, which is the equivalent of stashing American ballots in

the Kremlin. . . . [As] of today, what we see in terms of foreign interference in 2020 is going to make 2016 look like small potatoes. This is a national security issue! . . . The total lack of cybersecurity standards is especially troubling . . . But the lack of cybersecurity standards leads local officials to unwittingly buy overpriced, insecure junk. Insecure junk guarantees three things: a big payday for the election-tech companies, long lines on Election Day, and other hostile foreign governments can influence the outcome of elections through hacks."

97. In March of 2022, White House press secretary Jen Psaki said the Russian government in 2016 "hacked our election here" in the United States.

98. The following month, Dara Lindenbaum, a nominee to serve on the Federal Election Commission, testified before the Senate Rules and Administration Committee. Lindenbaum was asked about her role as an election lawyer representing Stacey Abrams's campaign for governor of Georgia in 2018. Lindenbaum acknowledged she had alleged voting machines were used to illegally switch votes from one candidate to another during the 2018 election in Georgia. [20]

99. Dominion presented its Democracy Suite 5.5-A voting system to the State of Texas for certification to be used in public elections in Texas. In January 2019, the State of Texas rejected Dominion's application and refused to certify Democracy Suite 5.5-A. On October 2 and 3, 2019, Dominion presented Democracy Suite 5.5-A to the State of Texas for examination a second time, seeking certification for use in public elections in Texas. Again,

[20] PN1758 — Dara Lindenbaum — Federal Election Commission, https://www.congress.gov/nomination/117th-congress/1758; https://www.youtube.com/watch?v=wCPLL_D_spc

Democracy Suite 5.5-A failed the test. On January 24, 2020, the Texas Secretary of State denied certification of the system for use in Texas elections.

100. The experts designated by Texas to evaluate Democracy Suite 5.5-A flagged risk from the system's connectivity to the internet despite "vendor claims" that the system is "protected by hardening of data and IP address features," stating, "[T]he machines could be vulnerable to a rogue operator on a machine if the election LAN is not confined to just the machines used for the election . . . The ethernet port is active on the ICX BMD during an election. . . . This is an unnecessary open port during the voting period and could be used as an attack vector." Other security vulnerabilities found by Texas include use of a "rack mounted server" which "would typically be in a room other than a room used for the central count" and would present a security risk "since it is out of sight." In summary, "The examiner reports identified multiple hardware and software issues . . . . Specifically, the examiner reports raise concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and accurately; and is safe from fraudulent or unauthorized manipulation."

101. The Texas Attorney General explained, "We have not approved these voting systems based on repeated software and hardware issues. It was determined they were not accurate and that they failed — they had a vulnerability to fraud and unauthorized manipulation."

102. Dominion's DVS 5.5-B voting system, set to be used in the Midterm Election in Arizona, is substantially similar to the 5.5-A system that twice failed certification in Texas.

103. Though Texas did certify ES&S electronic voting machines for use in Texas, ES&S voting systems are, like Dominion's voting systems, opaque, easily hacked, and vulnerable to incorporation of compromised components through ES&S's supply chain.

E. Electronic Voting Machine Companies Have Not Been Transparent Concerning Their Systems

104. Election officials and voting system manufacturers have publicly denied that their election equipment is connected to the internet in order to assert the equipment is not susceptible to attack via a networked system.[21]

105. John Poulous, the CEO of Dominion Voting Systems, testified in December 2020 that Dominion's election systems are "closed systems that are not networked meaning they are not connected to the internet." This is false.

106. In a May 2016 interview, Dominion Vice President Goran Obradovic stated, "All devices of the ImageCast series have additional options such as modems for wireless and wired transfer of results from the very polling place…."[22] During the 2020 election Dominion election equipment was connected to the internet when it should not have been.[23] A Dominion representative in Wayne County, Michigan stated that during the voting in the 2020 election

---

[21] Kim Zetter, *Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials*, Vice (Aug. 8, 2019) (https://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials).

[22] Economy & Business, Interview: How do the others do this? A technological solution exists for elections with complete security, privacy, and transparency pp.30, 31 (May 2016) (https://ekonomijaibiznis.mk/ControlPanel/Upload/Free_Editions/wZ0X5bz60KCgpcvFcEBvA/maj%202016%20ENG/mobile/index.html#p=31).

[23] Aff. of Patrick J. Colbeck, *Costantino v. City of Detroit*, no. 20-014780-AW (Wayne Co., Mich. Cir. Ct. Nov. 8, 2020).

there were irregularities with Dominion's election equipment, including that equipment was connected to the internet and equipment had scanning issues.

107. On Monday, November 2, 2020, the day before the 2020 election, Dominion uploaded software updates into election equipment that Dominion had supplied in the United States.[24] These software updates were unplanned and unannounced. In some counties in Georgia, Dominion's software update caused election equipment to malfunction the next day during the election. The supervisor of one County Board of Elections stated that Dominion "uploaded something last night, which is not normal, and it caused a glitch," and "[t]hat is something that they don't ever do. I've never seen them update anything the day before the election." Dominion had earlier publicly denied that any updates just prior to election day were made and that its election equipment was connected to the internet—both of which were false statements.[25]

108. In December 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Agency ("CISA") revealed that malicious hackers had compromised and exploited SolarWinds Orion network management software products.[26] On April 15, 2021, the White

[24] Kim Zetter, *Cause of Election Day Glitch in Georgia Counties Still Unexplained*, Politico (Nov. 12, 2020) (https://www.politico.com/news/2020/11/04/georgia-election-machine-glitch-434065).

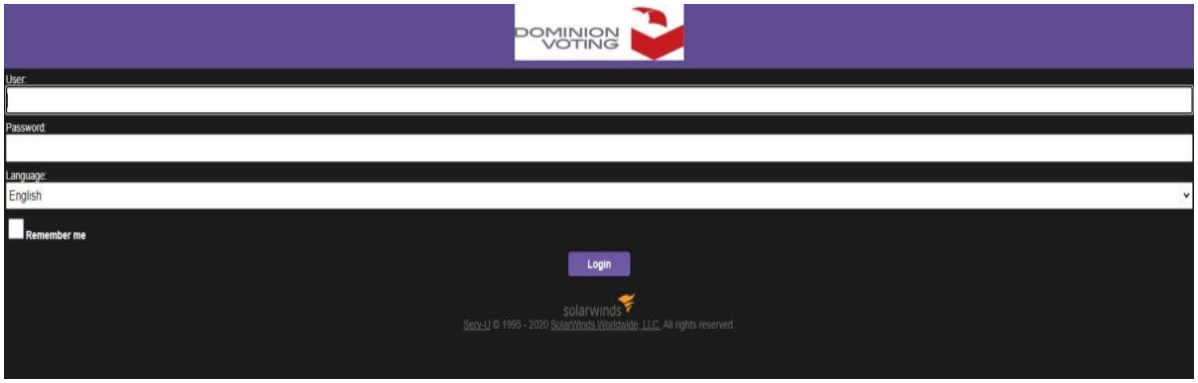
[25] Isabel van Brugen, *Dominion Voting Machines Were Updated Before Election, Georgia Official Confirms*, The Epoch Times (Dec. 4, 2020) (https://www.theepochtimes.com/dominion-voting-machines-were-updated-before-election-georgia-official-confirms_3604668.html).

[26] CISA, *CISA issues emergency directive to mitigate the compromise of SolarWinds Orion network management products* (Dec. 14, 2020) (https://www.cisa.gov/news/2020/ 12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network).

House announced imposition of sanctions on Russia in response to Russian "malicious cyber activities, such as the SolarWinds incident."[27]

109. Dominion CEO John Poulos stated that Dominion did not use SolarWinds.

110. Dominion in fact did use SolarWinds. Dominion's website formerly displayed a SolarWinds logo, but that logo was removed.



111. Dominion refuses to provide access to allow the public to forensically investigate its "proprietary" software, machines, and systems, to determine whether its election equipment is secure, has been hacked, or has malware installed.

112. No electronic voting system to be used in Arizona in the Midterm Election employs "open source" technology, which is electronic equipment for which the details of the components of the system, including its software, is published and publicly accessible. Though Dominion and E&S do not offer open source voting technology, it has been available to Defendants from other vendors for years.

[27] The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government* (Apr. 15, 2021) (https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/).

113. Defendants have failed or refused to institute open source voting technologies in Arizona, even though such technology would promote both security and transparency, as voters and office-seekers throughout Arizona would know the specific risks to, or manipulation of, election results.

114. This lack of transparency by electronic voting machine companies has created a "black box" system of voting which lacks credibility and integrity.

F. Irregularities and Evidence of Illegal Vote Manipulations in Electronic Voting Systems During the 2020 General Election Have Been Found

115. Evidence has been found of illegal vote manipulation on electronic voting machines during the 2020 election.

116. Dominion Democracy Suite software was used to tabulate votes in 62 Colorado counties, including Mesa County and Elbert County, during the 2020 election. Subsequent examination of equipment from Mesa County and Elbert County showed the Democracy Suite software created unauthorized databases on the hard drive of the election management system servers. On March 21, 2022, electronic database expert Jeffrey O'Donnell and computer science expert Dr. Walter Daugherty published a report concluding that ballots were manipulated in the unauthorized databases on the Mesa County server during Colorado's November 2020 and April 2021 elections.

117. On February 28, 2022, and after a comprehensive review of the Dominion systems used in Colorado, cybersecurity expert Douglas Gould published a report concluding that the system was "configured to automatically overwrite log files that exceed 20 MB, thereby

violating federal standards that require the preservation of log files," that it was configured "to allow any IP address in the world to access the SQL service port, (1433), which violates 2002 VSS security standards," and that it "uses generic user IDs and passwords and a common shared password, some of which have administrative access," in violation of 2002 VSS security standards.

118. Electronic forensic experts examined equipment used in Michigan to administer voting during the 2020 election and concluded the equipment had been connected to the internet, either by Wi-Fi or a LAN wire, that there were multiple ways the election results could have been modified without leaving a trace; and the same problems have been around for 10 years or more. One expert "examined the forensic image of a Dominion ICX system utilized in the November 2020 election and discovered evidence of internet communications to a number of public and private IP addresses."

119. In Wisconsin, during the voting in the 2020 election, Dominion election equipment that was not supposed to be connected to the internet was connected to a "hidden" Wi-Fi network.[28]

120. In April 2021, the Biden administration announced sanctions against Russia for election interference and hacking in the 2020 United States presidential election.[29]

[28] M.D. Kittle, *Emails: Green Bay's 'Hidden' Election Networks*, Wisconsin Spotlight (Mar. 21, 2021) (https://wisconsinspotlight.com/emails-green-bays-hidden-election-networks/).
[29] Natasha Truak and Amanda Macias, *Biden administration slaps new sanctions on Russia for cyberattacks, election interference*, CNBC (Apr. 16, 2021) (https://www.cnbc.com/2021/04/15/biden-administration-sanctions-russia-for-cyber-attacks-election-interference.html).

121. Following the 2020 election, lawmakers in multiple states initiated investigations and audits of the results.

122. The Arizona Senate hired a team of forensic auditors to review Maricopa County's election process. The auditors issued a partial audit report on September 24, 2021, which found: (1) "None of the various systems related to elections had numbers that would balance and agree with each other. In some cases, these differences were significant"; (2) "Files were missing from the Election Management System (EMS) Server"; (3) "Logs appeared to be intentionally rolled over, and all the data in the database related to the 2020 General Election had been fully cleared"; (4) "Software and patch protocols were not followed"; and (5) basic cyber security best practices and guidelines from the CISA were not followed.[30]

123. Retired Wisconsin Supreme Court Justice Michael Gableman conducted an investigation of the 2020 election in Wisconsin at the direction of the Wisconsin Assembly. Gableman issued a report in March 2022 noting that "at least some machines had access to the internet on election night."[31] He concluded that several machines manufactured by ES&S and used in the 2020 election in Wisconsin were "made with a 4G wireless modem installed, enabling them to connect to the internet through a Wi-Fi hotspot."

---

[30] *Maricopa County Forensic Election Audit, Volume I,* pp.1-3 (Sept. 24, 2021) (available at https://c692f527-da75-4c86-b5d1-8b3d5d4d5b43.filesusr.com/ugd/2f3470_a91b5cd3655445b498f9acc63db35afd.pdf).

[31] Office of the Special Counsel: Second Interim Investigative Report On the Apparatus & Procedures of the Wisconsin Elections System, March 1, 2022, p. 13.

124. During a December 30, 2020 live-streamed hearing held by the Georgia Senate Judiciary Subcommittee on Elections, an expert witness testified that an active Dominion polling pad had been hacked and the intrusion was being maintained even as he was speaking.[32]

G. Arizona's Voting Systems Do Not Comply with State or Federal Standards

125. All voting systems and voting equipment used in Arizona must comply with standards set forth in Federal Election Commission Publication "2002 Voting Systems Standards" ("2002 VSS"). A.R.S. § 16-442(B).

126. The 2002 VSS standards require that all electronic voting systems shall:

> g. Record and report the date and time of normal and abnormal events;
>
> h. Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.)
>
> i. Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator;
>
> [VSS, § 2.2.4.1]
>
> …
>
> a. Maintain the integrity of voting and audit data during an election, and for at least 22 months thereafter, a time sufficient in which to resolve most contested elections and support other activities related to the reconstruction and investigation of a contested election; and
>
> b. Protect against the failure of any data input or storage device at a location controlled by the jurisdiction or its contractors, and against any attempt at improper data entry or retrieval.
>
> [VSS, § 4.3]

[32] Hearing of Georgia Senate Judiciary Subcommittee on Elections, Dec. 30, 2020 (https://www.youtube.com/watch?v=D5c034r0RlU beginning at 4:07:58).

127. Defendant Hobbs has statutory duties to test, certify, and qualify software and hardware that is used on county election systems. A.R.S. § 16-442(B). Defendant Hobbs certified Dominion's DVS 5.5-B voting system for use in Arizona on or around November 5, 2019. The DVS 5.5-B system includes the Dominion ImageCast Precent2 ("ICP2").

128. ICP2 does not meet 2002 VSS standards or Arizona's statutory requirements. It is normally configured with cellular wireless connections, Wi-Fi access and multiple wired LAN connections, each of which provide an access point for unauthorized remote connection and thereby make it impossible to know whether improper data entry or retrieval has occurred or whether the equipment has preserved election records unmodified or not, in violation of the standards. The ICP permits software scripts to run which cause the deletion of election log file entries, thereby failing to preserve records of events which the standards require to be recorded. The ICP permits election files and folders to be deleted, in violation of the standards.

129. University of Michigan Professor of Computer Science and Engineering J. Alex Halderman performed a thorough examination of voting equipment used in Georgia, which is also used in Arizona. In a series of expert reports submitted in litigation still pending in the Northern District of Georgia, Professor Halderman stated that this voting equipment can be manipulated "to steal votes," has "numerous security vulnerabilities" that "would allow attackers to install malicious software" through either "temporary physical access (such as that of voters in the polling place) or remotely from election management systems." He stated that these "are not general weaknesses or theoretical problems, but rather specific flaws" which he was "prepared to demonstrate proof-of-concept malware that can exploit them to steal votes."

He also concluded that the equipment "is very likely to contain other, equally critical flaws that are yet to be discovered." He specifically noted that this same equipment, the ICX, will be used in 2022 in "for accessible voting in Alaska and large parts of Arizona . . ."

130. In the Midterm Election, Arizona intends to use, in part, the same software about which Dr. Halderman testified. The ICX fails to meet VSS standards for the reasons stated in Dr. Halderman's reports.

131. By falling short of VSS standards, DVS 5.5-B is noncompliant with Arizona or federal law and should not have been certified for use.

132. By seeking to use DVS 5.5-B in the Midterm Election, Defendant intends to facilitate violations of Arizona law and federal law.

133. By choosing to continue using the non-compliant system in the Midterm Election without taking any meaningful steps to remedy known security breaches affecting Arizona voters, Defendants know that they will cause voters to cast votes in Midterm Election on an inaccurate, vulnerable and unreliable voting system that cannot produce verifiable results and does not .pass constitutional or statutory muster.

H. Arizona's Audit Regime is Insufficient to Negate Electronic Voting Machines' Vulnerabilities

134. Post-election audits do not and cannot remediate the security problems inherent in the use of electronic voting machines.

135. All post-election audit procedures can be defeated by sophisticated manipulation of electronic voting machines.

136. Dr. Halderman stated in a Declaration dated August 2, 2021, that malware can defeat "all the procedural protections practiced by [Georgia], including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs)." Dr. Halderman testified that the voting system at issue in Georgia is used in fifteen other states, including Arizona.

137. Electronic voting systems vendors have repeatedly refused to comply with post-election audits, diminishing the audits' ability to yield reliable conclusions about the validity of the election results.

138. On July 26, 2021, Arizona Senate leaders issued subpoenas to Dominion Voting Systems in connection with the Senate's audit of the 2020 election in Maricopa County, Arizona. Among other materials, the July 26 subpoenas sought production of usernames, passwords, tokens, and pins to the ballot tabulation machines the Maricopa County rents from Dominion, including all that would provide administrative access.

139. Dominion flatly refused to comply with this validly-issued legislative subpoena. In a letter to Senate President Karen Fann, Dominion wrongly claimed the subpoena seeking credentials necessary to access the Dominion voting systems to validate an election "violat[ed] [Dominion's] constitutional rights and … exceed[ed] the Legislature's constitutional and statutory authority" and that responding to the subpoena would "cause grave harm" to Dominion.

140. ES&S has similarly flouted legislative subpoenas in Wisconsin. In a letter dated January 21, 2022, ES&S responded to a Wisconsin subpoena with a letter erroneously asserting

it "is under no obligation to respond," despite the fact the subpoena was issued by the state Senate.

141. Any voting system that relies on the hidden workings of electronic devices in the casting and/or counting of the vote is a system of which voters may reasonably be suspicious. Post-election audits are not sufficient to alleviate their reasonable suspicions because voting machine manufacturers have demonstrated that they will not provide the information necessary to audit an election.

142. To restore legitimacy to Arizona's election regime for all voters, regardless of party, and to comply with constitutional and legal requirements, a secure and feasible alternative must supplant reliance on faulty electronic voting systems.

I. Voting on Paper Ballots and Counting Those Votes by Hand Is the Most Effective and Presently the Only Secure Election Method

143. Plaintiffs seek for the Court to Order, an election conducted by paper ballot, as an alternative to the current framework. To satisfy constitutional requirements of reliability, accuracy, and security, the following is a summary of procedures that should be implemented:

- Ballots are cast by voters filling out paper ballots, by hand. The ballots are then placed in a sealed ballot box. Each ballot bears a discrete, unique identification number, which is made known by election officials only to the voter, so that the voter can later verify whether his or her ballot was counted properly. All ballots will be printed on specialized paper to confirm their authenticity.

- Though a uniform chain of custody, ballot boxes are conveyed to a precinct level counting location while still sealed.

- With party representatives, ballot boxes are unsealed, one at a time, and ballots are removed and counted in batches of 100, then returned to the ballot box. When all ballots in a ballot box have been counted, the box is resealed, with a copy of the batch tally sheets left inside the box, and the batch tally sheets carried to the tally center with a uniform chain of custody.

- Ballots are counted, one at a time, by three independent counters, who each produce a tally sheet that is compared to the other tally sheets at the completion of each batch.

- At the tally center, two independent talliers add the counts from the batch sheets, and their results are compared to ensure accuracy.

- Vote counting from paper ballots is conducted in full view of multiple, recording, streaming cameras that ensure a) no ballot is ever touched or accessible to anyone off-camera or removed from view between acceptance of a cast ballot and completion of counting, b) all ballots, while being counted are in full view of a camera and are readable on the video, and c) batch tally sheets and precinct tally sheets are in full view of a camera while being filled out and are readable on the video.

- Each cast ballot, from the time of receipt by a sworn official from a verified, eligible elector, remains on video through the completion of precinct counting and reporting.

- The video be live-streamed for public access and archived for use as an auditable record, with public access to replay a copy of that auditable record.

- Anonymity will be maintained however, any elector will be able to identify their own ballot by the discrete, serial ballot number known only to themselves, and to see that their own ballot is accurately counted

144. Every county in Arizona, regardless of size, demographics, or any other ostensibly unique characteristic, can simply and securely count votes cast on paper ballots without using centralized machine-counting or computerized optical scanners.

145. The recent hand count in Maricopa County, the second largest voting jurisdiction in the United States, offers Defendant Hobbs a proof-of-concept and a superior alternative to relying on corruptible electronic voting systems. Voting jurisdictions larger than any within Arizona, including France and Taiwan, have also proven that hand-count voting can deliver swift, secure, and accurate election results.

J. Past and Threatened Conduct of Defendant Hobbs

146. Defendant Hobbs is, in her capacity as Secretary of State, charged by statute with carrying out the following duties:

- "After consultation with each county board of supervisors or other officer in charge of elections, the secretary of state shall prescribe rules to achieve and maintain the maximum degree of correctness, impartiality, uniformity and efficiency on the procedures for early voting and voting, and of producing, distributing, collecting, counting, tabulating and storing ballots."

A.R.S. § 16-452 (A).

- "The secretary of state shall provide personnel who are experts in electronic voting systems and procedures and in electronic voting system security to field check and review electronic voting systems and recommend needed statutory and procedural changes."

A.R.S. § 16-452 (D).

147. Defendant Hobbs, in her capacity as Secretary of State, is further charged with ensuring that electronic voting systems used throughout Arizona meet the following requirements:

- "Be suitably designed for the purpose used and be of durable construction, and may be used safely, efficiently and accurately in the conduct of elections and counting ballots…"
- "When properly operated, record correctly and count accurately every vote cast…" and
- "Provide a durable paper document that visually indicates the voter's selections, that the voter may use to verify the voter's choices, that may be spoiled by the voter if it fails to reflect the voter's choices and that permits the voter to cast a new ballot."

A.R.S. § 16-446 (B).

148. Defendant Hobbs, in her capacity as Secretary of State, is further charged with ensuring that all computer election programs filed with the office of the Secretary of State shall be used by the Secretary of State or Attorney General to preclude fraud or any unlawful act. A.R.S. § 16-445(D).

149. By certifying deficient electronic voting systems for use in past elections, Defendant Hobbs has failed to meet these duties set forth above.

150. Defendant Hobbs, acting in her official capacity as the Secretary of State, has shown her intention to require the use of electronic voting systems for all Arizona voters in the Midterm Election.

151. In so doing, Defendant Hobbs will violate her duties under A.R.S. § 16-442(B), and violate the Constitutional rights of Plaintiffs and all voters in the State of Arizona.

K. Past and Threatened Conduct of Maricopa Defendants and Pima Defendants

152. The Maricopa Defendants and Pima Defendants, acting in their official capacity, are charged with the duty to:

- "[e]stablish, abolish and change election precincts, appoint inspectors and judges of elections, canvass election returns, declare the result and issue certificates thereof…";
- "[a]dopt provisions necessary to preserve the health of the county, and provide for the expenses thereof";
- "[m]ake and enforce necessary rules and regulations for the government of its body, the preservation of order and the transaction of business."

A.R.S. § 11-251.

153. The Maricopa Defendants and Pima Defendants, acting in their official capacity, are charged with the duty to consult with Defendant Hobbs in order for Defendant Hobbs to "prescribe rules to achieve and maintain the maximum degree of correctness, impartiality, uniformity and efficiency on the procedures for early voting and voting, and of producing, distributing, collecting, counting, tabulating and storing ballots." A.R.S. § 16-452 (A).

154. The Maricopa Defendants and Pima Defendants have, in the past, failed in the duties set forth above by failing to, among other things, ensure that:

- operating systems and antivirus definitions of electronic voting systems were properly updated;
- electronic election files and security logs were preserved;
- election management servers were not connected to the Internet;
- access to election equipment was limited to authorized personnel; and
- communications over the system network were properly monitored.

155. The Maricopa Defendants and Pima Defendants intend to rely on the use of deficient electronic voting systems in the Midterm Election.

L. Imminent Injury

156. Plaintiff Lake seeks the office of Governor of the State of Arizona.

157. To gain that office, Plaintiff Lake must prevail in the Midterm Election, in which all votes will be tabulated, and many votes will be cast, on electronic voting systems.

158. Plaintiff Lake intends to vote in the Midterm Election in Arizona. To do so, she will be required to cast her vote, and have her vote counted, through electronic voting systems.

159. Plaintiff Finchem seeks the office of Secretary of State of the State of Arizona.

160. To gain that office, Plaintiff Finchem must prevail in the Midterm Election, in which all votes will be tabulated, and many votes will be cast, on electronic voting systems.

161. Plaintiff Finchem intends to vote in the Midterm Election in Arizona. To do so, he will be required to cast his vote, and have his vote counted, through electronic voting systems.

162. All persons who vote in the Midterm Election, if required to vote using an electronic voting system or have their vote counted using an electronic voting system, will be irreparably harmed because the voting system does not reliably provide trustworthy and verifiable election results. The voting system therefore burdens and infringes their fundamental right to vote and have their vote accurately counted in conjunction with the accurate counting of all other legal votes, and *only* other legal votes.

163. Any voter who votes using a paper ballot will be irreparably harmed in the exercise of the fundamental right to vote if his or her vote is tabulated together with the votes of other voters who cast ballots using an unreliable, untrustworthy electronic system.

164. Any voter will be irreparably harmed in the exercise of the constitutional, fundamental right to vote if he or she is required to cast a ballot using – or in an election in which anyone will use – an electronic voting system, or if his or her ballot is tabulated using an electronic voting system.

165. Each of the foregoing harms to Plaintiff is imminent for standing purposes because the Midterm Election is set to occur on a fixed date not later than eight months after the date when this action is to be filed.

166. No Plaintiff can be adequately compensated for these harms in an action at law for money damages brought after the fact because the violation of constitutional rights is an irreparable injury.

IV. CLAIMS

COUNT I: VIOLATION OF DUE PROCESS

(*Seeking declaratory and injunctive relief against all Defendants*)

167. Plaintiffs incorporate and each and every preceding paragraph in this Complaint.

168. The right to vote is a fundamental right protected by the Due Process Clause of the Fourteenth Amendment of the U.S. Constitution and Article 2, Section 4 of the Arizona Constitution.

169. The fundamental right to vote encompasses the right to have that vote counted accurately, and it is protected by the Due Process Clause of the Fourteenth Amendment of the U.S. Constitution and Article 2, Section 4 of the Arizona Constitution.

170. Defendants have violated Plaintiffs' fundamental right to vote by deploying an electronic voting equipment system that has:

(a) Failed to provide reasonable and adequate protection against the real and substantial threat of electronic and other intrusion and manipulation by individuals and entities without authorization to do so;

(b) Failed to include the minimal and legally required steps to ensure that such equipment could not be operated without authorization; to provide the minimal and legally required protection for such equipment to secure against unauthorized tampering; to test, inspect, and seal, as required by law, the equipment to ensure that each unit would count all votes cast and that no votes that were not properly cast would not be counted; and to ensure that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as required by law;

(c) Failed to provide a reasonable and adequate method for voting by which Arizona electors' votes would be accurately counted.

171. By choosing to move forward in using an unsecure system, Defendants willfully and negligently abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an illegal and unreliable system--a system that must be presumed to be compromised and incapable of producing verifiable results.

172. Despite Defendants' knowledge that electronic voting systems used in Arizona do not comply and cannot be made to comply with state and federal law, Defendants plan to continue to use these non-compliant systems in the Midterm Election.

173. Plaintiffs ask this Court to declare that these Defendants violated the Due Process Clause of the Fourteenth Amendment of the United States Constitution and Article 2, Section 4 of the Arizona Constitution; enjoin Defendants' use of electronic voting systems for future elections; and award attorneys' fees and costs for Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast was thwarted.

COUNT II: VIOLATION OF EQUAL PROTECTION
(*Seeking declaratory and injunctive relief against all Defendants*)

174. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

175. By requiring Plaintiffs to vote using electronic voting systems in the Midterm Election which are unsecure and vulnerable to manipulation and intrusion there will be an unequal voting tabulation of votes treating Plaintiffs who vote in Arizona differently than other, similarly situated voters who cast ballots in the same election.

176. These severe burdens and infringements that Defendants will impose unequally on Plaintiffs who vote through an electronic voting system will violate the Equal Protection Clause of the Fourteenth Amendment.

177. These severe burdens and infringements that will be caused by Defendants' conduct are not outweighed or justified by, and are not necessary to promote, any substantial or compelling state interest that cannot be accomplished by other, less restrictive means, like conducting the Midterm Election using hand counted paper ballots.

178. Requiring voters to be deprived of their constitutional right to equal protection of the laws as a condition of being able to enjoy the benefits and conveniences of voting in person at the polls violates the unconstitutional conditions doctrine.

179. Unless Defendants are enjoined by this Court, then Plaintiffs will have no adequate legal, administrative, or other remedy by which to prevent or minimize the irreparable, imminent injury that is threatened by Defendants intended conduct. Accordingly, injunctive relief against these Defendants is warranted.

COUNT III: VIOLATION OF FUNDAMENTAL RIGHT TO VOTE
(*Seeking declaratory and injunctive relief against all Defendants*)

180. Plaintiffs incorporate and each and every preceding paragraph in this Complaint.

181. The right to vote is a fundamental right protected by the U.S. Constitution. *See, e.g., Reynolds v. Sims*, 377 U.S. 533, 561-62 (1964).

182. The fundamental right to vote encompasses the right to have that vote counted accurately. *See, e.g., United States v. Mosley,* 238 U.S. 383, 386 (1915).

183. Defendants have violated Plaintiffs' fundamental right to vote by deploying an electronic voting equipment system that has:

(a) Failed to provide reasonable and adequate protection against the real and substantial threat of electronic and other intrusion and manipulation by individuals and entities without authorization to do so;

(b) Failed to include the minimal and legally required steps to ensure that such equipment could not be operated without authorization; to provide the minimal and legally required protection for such equipment to secure against unauthorized tampering; to test, inspect,

and seal, as required by law, the equipment to ensure that each unit would count all votes cast and that no votes that were not properly cast would not be counted; and to ensure that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as required by law;

(c) Failed to provide a reasonable and adequate method for voting by which Arizona electors' votes would be accurately counted.

184. By choosing to move forward in using the non-compliant system, Defendants have abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an illegal and unreliable system--a system that is unsecure and vulnerable to manipulation and intrusion and incapable of producing verifiable results.

185. Defendants' violation of the Due Process Clause is patently and fundamentally unfair and therefore relief is warranted. Accordingly, Plaintiffs ask this Court to declare that these Defendants violated the Due Process Clause of the Fourteenth Amendment of the United States Constitution and Article 2, Section 4 of the Arizona Constitution; enjoin Defendants' use of electronic voting systems for future elections; and award attorneys' fees and costs for Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast was thwarted.

COUNT IV: CIVIL ACTION FOR DEPRIVATION OF RIGHTS UNDER 42 U.S.C. § 1983

(*Seeking declaratory and injunctive relief against all Defendants*)

186. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

187. The foregoing violations will occur as a consequence of Defendants acting under color of state law. Accordingly, Plaintiffs bring this cause of action for prospective equitable relief against Defendants pursuant to 42 U.S.C. § 1983.

188. By requiring the citizens of Arizona to vote using a system which may miscount their votes, the Defendants will violate the rights of the citizens' under the Constitution of the United States.

189. Unless Defendants are enjoined by this Court, then Plaintiffs will have no adequate legal, administrative, or other remedy by which to prevent or minimize the irreparable, imminent injury that is threatened by Defendants' intended conduct. Accordingly, appropriate damages and injunctive relief against these Defendants is warranted.

COUNT V: VIOLATION OF A.R.S. § 11-251
(Against Maricopa Defendants and Pima Defendants)

190. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

191. Maricopa Defendants and Pima Defendants, as members of the Maricopa Board and the Pima Board, are charged with statutory duties to electors in Arizona, including Plaintiffs, under A.R.S. § 11-251.

192. Maricopa Defendants and Pima Defendants have failed to meet the duties set forth in A.R.S. § 11-251 to adopt provisions necessary to preserve the health of Maricopa County and Pima County.

193. Maricopa Defendants and Pima Defendants have failed to meet the duties set forth in A.R.S. § 11-251 to make and enforce necessary rules and regulations for the government of

Maricopa County and Pima County or to the preserve the of order and the transaction of business.

194. Maricopa Defendants and Pima Defendants intend to continue in their failure to meet these duties through the Midterm Election.

195. Plaintiffs have a private right of action against Maricopa Defendants and Pima Defendants under Arizona law.

196. Unless Maricopa Defendants and Pima Defendants are enjoyed by this Court, then Plaintiffs will have not adequate administrative, or other remedy by which to prevent or minimize the irreparable, imminent injury that is threatened by the intended conduct of Maricopa Defendants and Pima Defendants. Accordingly, injunctive relief against these Defendants is warranted.

COUNT VI: DECLARATORY JUDGMENT - 28 U.S. CODE § 2201
(*Against All Defendants)*

197. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

198. Defendants' conduct will have the effect of violating the rights of the citizens of Arizona, as described above.

199. The Court has the authority pursuant to 28 U.S.C. § 2201 to issue an Order enjoining the State from conducting an election in which the votes are not accurately or securely tabulated.

200. If the State of Arizona is allowed to proceed with an election as described above, it will violate the rights of the citizens of the State by conducting an election with an unsecure, vulnerable electronic voting system which is susceptible to manipulation and intrusion.

201. Because of the above-described issues regarding the election system to be used by Defendants, the Court should issue an Order enjoining the State from using any electronic voting system unless and until the system is made open to the public and subjected to scientific analysis to determine whether it is absolutely secure from manipulation or intrusion.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

1. Enter a judgment finding and declaring it unconstitutional for any public election to be conducted using any model of electronic voting system to cast or tabulate votes.

2. Enter a preliminary and permanent injunction prohibiting Defendants from requiring or permitting voters to have votes cast or tabulated using any electronic voting system.

3. Enter an Order directing Defendants to conduct the Midterm Election consistent with the summary of procedures set forth in paragraph 140 of this Complaint.

4. Retain jurisdiction to ensure Defendants' ongoing compliance with the foregoing Orders.

5. Grant Plaintiffs an award of its reasonable attorney's fees, costs, and expenses incurred in this action pursuant to 42 U.S.C. § 1988.

6. Damages suffered by Plaintiffs to be determined at trial.

7. Grant Plaintiff such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all counts and issues so triable.

DATED: April 22, 2022.

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*
Andrew D. Parker (AZ Bar No. 028314)
888 Colwell Building
123 N. Third Street
Minneapolis, MN 55401
Telephone: (612) 355-4100
Facsimile: (612) 355-4101
parker@parkerdk.com

OLSEN LAW, P.C.

By */s/ Kurt Olsen*
Kurt Olsen (D.C. Bar No. 445279)*
1250 Connecticut Ave., NW, Suite 700
Washington, DC 20036
Telephone: (202) 408-7025
ko@olsenlawpc.com
* To be admitted *Pro Hac Vice*

Counsel for Plaintiffs Kari Lake and Mark Finchem

ALAN DERSHOWITZ CONSULTING LLC

By */s/ Alan M. Dershowitz*
Alan M. Dershowitz (MA Bar No. 121200)*
2255 Glades Road
Suite 321A
Boca Raton, FL 33431
* To be admitted *Pro Hac Vice*

Of Counsel for Plaintiffs Kari Lake and Mark Finchem