

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.

No. _____

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.

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.

1 2. Plaintiffs have a constitutional and statutory right to have their ballots, and all
2 ballots cast together with theirs, counted accurately and transparently, so that only legal votes
3 determine the winners of each office contested in the Midterm Election. Electronic voting
4 machines cannot be deemed reliably secure and do not meet the constitutional and statutory
5 mandates to guarantee a free and fair election. The use of untested and unverified electronic
6 voting machines violates the rights of Plaintiffs and their fellow voters and office seekers, and it
7 undermines public confidence in the validity of election results. Just as the government cannot
8 insist on “trust me,” so too, private companies that perform governmental functions, such as
9 vote counting, cannot be trusted without verification
10

11
12 3. Defendants each have duties to ensure elections held with a “maximum degree of
13 correctness, impartiality, uniformity and efficiency on the procedures for early voting and
14 voting, and of producing, distributing, collecting, counting, tabulating and storing ballots.”
15 A.R.S. § 16-452 (A). Defendants have fallen short of those duties, and they will do so again
16 unless this Court intervenes.
17

18 4. For two decades, experts and policymakers from across the political spectrum
19 have raised glaring failures with electronic voting systems. Indeed, just three months ago, a
20 computer science expert in *Curling v. Raffensperger*, Case No. 1:17-cv-02989-AT (U.S. Dist.
21 Ct., N.D. Ga.), identified catastrophic failures in electronic voting machines used in sixteen
22 states, including Arizona. The expert testified that the failures include the ability to defeat all
23 state safety procedures. This caused the Cybersecurity and Infrastructure Security Agency
24 (“CISA”) to enter an appearance and urge the federal district court to not allow disclosure of the
25
26

1 expert's report detailing these failures. The district court refused to allow disclosure of that
2 expert report to date. Secrecy destroys public confidence in our elections and election systems
3 that result in secrecy undermine our democratic process.
4

5 5. The problems with the electronic voting systems are not only technical, but
6 structural. To date, only three companies collectively provide voting machines and software for
7 90% of all eligible voters in the United States. Most of those machines are over a decade old,
8 have critical components manufactured overseas in countries, some of which are hostile to the
9 United States, and use software that is woefully outdated and vulnerable to catastrophic
10 cyberattacks. Indeed, countries like France have banned the use of electronic voting machines
11 due to lack of security and related vulnerabilities.
12

13 6. Given the limitations and flaws of existing technology, electronic voting machines
14 cannot legally be used to administer elections today and for the foreseeable future, unless and
15 until their current electronic voting system is objectively validated.
16

17 7. Through this Action, Plaintiffs seek an Order that Defendants collect and count
18 votes through a constitutionally acceptable process, which relies on tried and true precepts that
19 mandates integrity and transparency. This includes votes cast by hand on verifiable paper ballots
20 that maintains voter anonymity; votes counted by human beings, not by machines; and votes
21 counted with transparency, and in a fashion observable to the public.
22

23 8. It is important to note that this Complaint is not an attempt to undo the past. Most
24 specifically, it is not about undoing the 2020 presidential election. It is only about the future –
25 about upcoming elections that will employ voting machines designed and run by private
26

1 companies, performing a crucial governmental function, that refuse to disclose their software
2 and system components and subject them to neutral expert evaluation. It raises the profound
3 constitutional issue: can government avoid its obligation of democratic transparency and
4 accountability by delegating a critical governmental function to private companies?
5

6 I. INTRODUCTION

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

- 10 • Achieve and maintain the maximum degree of correctness, impartiality,
uniformity in elections.
- 11 • Ensure that all votes are counted safely, efficiently, and accurately.
- 12 • 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
13 unlawful act.
- 14 • Revoke the certification of electronic voting systems used in elections in Arizona.
- 15 • Demand access to the electronic voting system so that it can be examined by
objective experts.

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

18 11. Defendants Gates, Hickman, Sellers, Galvin, and Gallardo, as Members of the
19 Maricopa County Board of Supervisors, have caused the use of election systems and equipment
20 in Maricopa County that are rife with potentially glaring cybersecurity vulnerabilities, including
21

- 22 • Operating systems lacking necessary updates;
- 23 • Antivirus software lacking necessary updates;
- 24 • Open ports on the election management server, allowing for possible remote
25 access;
- 26

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

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

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

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

20 15. Some voters in Arizona will rely on electronic voting systems to cast their votes as
21 well as tabulate them. Voters who may have hearing or visual impairments may cast their votes
22
23
24
25
26

1 with the aid of electronic ballot marking devices manufactured primarily by ES&S or Dominion.
2 These voters' electoral choices are even more vulnerable to attack and manipulation, as ballot
3 marking devices pose significant security risks on their own.
4

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

8 17. Defendant Hobbs on or about November 5, 2019, certified the Dominion
9 Democracy Suite 5.5b voting system for use in elections held in Arizona. This voting system, as
10 well as the component parts identified above, will be used in the Midterm Election.
11

12 18. Defendant Hobbs after July 22, 2020, certified the ES&S ElectionWare 6.0.40
13 voting system, as well as its component parts, for use in elections held in Arizona. This voting
14 system, as well as the component parts identified above, will be used in the Midterm Election.¹
15

16 19. Defendant Hobbs's certification of the Dominion Democracy Suite 5.5b voting
17 system, as well as its component parts, was improper, absent objective evaluation.
18

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

21 21. Defendant Hobbs has the authority to revoke the certification of every voting
22 system, including all component parts thereto, certified by the State of Arizona. Defendant
23 Hobbs has improperly failed to exercise that authority.
24
25
26

¹ See <https://azsos.gov/elections/voting-election/voting-equipment>.

1 22. All optical scanners and ballot marking devices certified by Arizona, as well as the
2 software on which they rely, have been wrongly certified for use in Arizona. These systems are
3 potentially unsecure, lack adequate audit capacity, fail to meet minimum statutory requirements,
4 and deprive voters of the right to have their votes counted and reported in an accurate, auditable,
5 legal, and transparent process. Using them in the upcoming elections, without objective
6 validation, violates the voting rights of every Arizonan.
7

8 23. All electronic voting machines and election management systems, including those
9 slated to be used in Arizona in the Midterm Election, can be manipulated through internal or
10 external intrusion to alter votes and vote tallies.
11

12 24. Specific vulnerabilities in the electronic voting machines used by Maricopa
13 County have been explicitly identified and publicized in analyses by cybersecurity experts, even
14 absent access to the systems.
15

16 25. Substantially similar vulnerabilities in electronic voting machines in general have
17 been identified and publicized in analyses presented to various congressional committees. All
18 electronic voting machines can be connected to the internet or cellular networks, directly or
19 indirectly, at various steps in the voting, counting, tabulating, and/or reporting process.
20

21 26. Voting machines and systems used in Arizona contain electronic components
22 manufactured or assembled in foreign nations which have attempted to manipulate the results of
23 U.S. elections.
24
25
26

1 27. Electronic voting machines and software manufactured by industry leaders,
2 specifically including Dominion and ES&S, are vulnerable to cyberattacks before, during, and
3 after an election in a manner that could alter election outcomes.
4

5 28. These systems can be connected to the internet or cellular networks, which
6 provides an access point for unauthorized manipulation of their software and data. They often
7 rely on outdated versions of Windows, which lack necessary security updates. Both of these
8 common shortcomings leave the systems vulnerable to generalized, widespread-effect attacks.
9

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

12 30. Expert testimony demonstrates that all safety measures intended to secure
13 electronic voting machines against manipulation of votes, such as risk limiting audits and logic
14 and accuracy tests, can be defeated.
15

16 31. Other countries, including France and Taiwan, have completely or largely banned
17 or limited the use of electronic voting machines due to the security risks they present.
18

19 32. Arizona's electronic election infrastructure is potentially susceptible to malicious
20 manipulation that can cause incorrect counting of votes. Despite a nationwide bipartisan
21 consensus on this risk, election officials in Arizona continue to administer elections dependent
22 upon unreliable, insecure electronic voting systems. These officials, including Defendants in
23 Maricopa County, refuse to take necessary action to address known and currently unknown
24 election security vulnerabilities, and in some cases have obstructed court authorized inspections
25 of their electronic voting systems.
26

1 40. Plaintiff Finchem has standing to bring this action as an intended voter in the
2 Midterm Election and as a “qualified elector” under A.R.S. § 16-121. As a candidate for
3 Secretary of State of Arizona Plaintiff Finchem further has standing as an aggrieved person to
4 bring this action.
5

6 41. Defendant Hobbs is, through this Complaint, sued for prospective declaratory and
7 injunctive relief in her official capacity as the Secretary of State of Arizona, together with any
8 successor in office automatically substituted for Defendant Hobbs by operation of Fed. R. Civ.
9 P. 25(d).
10

11 42. In her official capacity, Defendant Hobbs is the chief election officer for the State
12 of Arizona. Defendant Hobbs is responsible for the orderly and accurate administration of public
13 election processes in the state of Arizona. This responsibility includes a statutory duty to ensure
14 that “satisfactorily tested” voting systems are used to administer public elections, A.R.S. § 16-
15 441, and to conduct any reexaminations of previously adopted voting systems, upon request or
16 at Defendant Hobbs’s own discretion.
17

18 43. Defendant Hobbs is further required by law to determine the voting equipment that
19 is to be used to cast and count the votes in all county, state, and federal elections in Arizona.
20 A.R.S. §§ 16-446, 16-452.
21

22 44. Defendants Bill Gates, Clint Hickman, Jack Sellers, Thomas Galvin, and Steve
23 Gallardo (collectively “Maricopa Defendants”) are sued for prospective declaratory and
24 injunctive relief in their official capacities as members of the Maricopa County Board of
25 Supervisors (“Maricopa Board”).
26

1 45. Defendants Scott, Heinz, Bronson, Christy, and Grijalva (collectively “Pima
2 Defendants”) are sued for prospective declaratory and injunctive relief in their official capacities
3 as members of the Pima County Board of Supervisors (“Pima Board”).
4

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

- 7
- 8 • “[e]stablish, abolish and change election precincts, appoint inspectors and judges
of elections, canvass election returns, declare the result and issue certificates thereof...”;
 - 9 • “[a]dopt provisions necessary to preserve the health of the county, and provide for
the expenses thereof”;
10
 - 11 • “[m]ake and enforce necessary rules and regulations for the government of its
body, the preservation of order and the transaction of business.”

12 **II. JURISDICTION AND VENUE**

13

14 47. Plaintiffs bring this action under 42 U.S.C. § 1983 and the cause of action
15 recognized in *Ex parte Young*, 209 U.S. 123 (1908), and its progeny to challenge government
16 officers’ “ongoing violation of federal law and [to] seek[] prospective relief” under the equity
17 jurisdiction conferred on federal district courts by the Judiciary Act of 1789.
18

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

22 49. This Court has supplemental jurisdiction over Plaintiffs’ claims under 28 U.S.C. §
23 1367.
24

25 50. This Court has authority to grant declaratory relief based on 28 U.S.C. §§ 2201 &
26 2202, and Rule 57 of the Federal Rules of Civil Procedure.

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

3
4 58. After the recount of the 2000 presidential election in Florida and the ensuing *Bush*
5 *v. Gore* decision, Congress passed the Help America Vote Act in 2002.³ In so doing, Congress
6 opened the proverbial spigot. Billions of federal dollars were spent to move states, including
7 Arizona, from paper-based voting systems to electronic, computer-based systems.

8
9 59. Since 2002, elections throughout the United States have increasingly and largely
10 been conducted using a handful of computer-based election management systems. These
11 systems are created, maintained, and administered by a small number of companies having little
12 to no transparency to the public, producing results that are far more difficult to audit than paper-
13 based systems, and lack any meaningful federal standards or security requirements beyond what
14 individual states may choose to certify. Leaders of both major parties have expressed concern
15 about this lack of transparency, analysis and accountability.

16
17 60. As of 2019, Dominion, ES&S, and one other company (Hart InterCivic) supplied
18 more than ninety percent of the nationwide “voting machine market.”⁴ Dominion and ES&S
19 control even more than that share of the market in Arizona. All three of these providers’
20 electronic voting machines can be hacked or compromised with malware, as has been
21 demonstrated by recognized computer science experts, including experts from the University of
22

23
24
25 ³ 52 U.S.C. § 20901 *et seq.*

26 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>).

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

5
6 61. This small cadre of companies supplies the hardware and software for the
7 electronic voting machines, in some cases manages the voter registration rolls, maintains the
8 voter records, partially manages the elections, programs the vote counting, and reports the
9 election results.
10

11 62. Jurisdictions throughout the nation, including Arizona, have functionally
12 outsourced all election operations to these private companies. In the upcoming Midterm
13 Election, over three thousand counties across the United States will have delegated the
14 governmental responsibility for programming and administering elections to private contractors.
15

16 63. This includes all counties in Arizona, most of which have contracted with
17 Dominion or ES&S to provide machines, software, and services for the Midterm Election. For
18 example, in Defendant Maricopa County, officials do not possess credentials necessary to
19 validate tabulator configurations and independently validate the voting system prior to an
20 election. Dominion maintains those credentials.
21

22 64. By its own account, Dominion provides an “End-To-End Election Management
23 System” that “[d]rives the entire election project through a single comprehensive database.”⁵ Its
24

25
26

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

1 tools “build the election project,” and its technology provides “solutions” for “voting &
2 tabulation,” and “tallying & reporting,” and “auditing the election.” The products sold by
3 Dominion include ballot marking machines, tabulation machines, and central tabulation
4 machines, among others.
5

6 65. Dominion, in its normal course of business, including the Midterm Election in
7 Arizona, manufactures, distributes, and maintains voting hardware and software. Dominion also
8 executes software updates, fixes, and patches for its voting machines and election management
9 systems.
10

11 66. After votes are tabulated at the county level using Dominion’s electronic election
12 management system in the Midterm Election, the vote tallies will be uploaded over the internet
13 to an election reporting system.
14

15 67. Dominion’s machines and systems range from the “election event designer”—
16 software that creates the ballots voters will mark while voting, as well as programing the
17 tabulators of those votes—to the devices on which voters mark their votes (“ballot marking
18 devices,” or “BMDs”), to the machines that tabulate the votes at the precinct level, to the
19 machines that receive and tabulate the various precinct results (“centralized tabulation”), to the
20 systems and options for transmitting those results from the BMD to the precinct tabulator to the
21 central tabulator to, ultimately, the official government authority responsible for certifying the
22 election results. In the Midterm Election, many Arizonans will cast their votes on Dominion
23 BMDs, while nearly *all* Arizonans will have their votes tabulated with Dominion machines.
24
25
26

1 68. Dominion controls the administration and conduct of the elections in those
2 jurisdictions where its systems are deployed, including Arizona. Any vulnerabilities or
3 weaknesses in Dominion’s systems, at the very least, call into question the integrity and
4 reliability of all election results coming from those jurisdictions. Dominion has refused to
5 disclose its software and other parts of its electronic voting system in order to subject it to neutral
6 expert evaluation.
7

8 69. As an example, following the 2020 election an audit of election processes and
9 results in Maricopa County, Arizona was ordered. It was concluded that:
10

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

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

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

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

26 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

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

3
4 71. With each passing election the unreliability of electronic voting machines has
5 become more apparent. In light of this experience, the vote tallies reported by electronic voting
6 machines cannot, without objective evaluation, be trusted to accurately show which candidates
7 actually received the most votes.

8
9 72. Credible allegations of electronic voting machine “glitches” that materially
10 impacted specific races began to emerge in 2002. *Black Box Voting*, the seminal publication
11 documenting early pitfalls of electronic voting systems, chronicles the following failures:

12 In the Alabama 2002 general election, machines made by Election Systems and
13 Software (ES&S) flipped the governor’s race. Six thousand three hundred Baldwin
14 County electronic votes mysteriously disappeared after the polls had closed and everyone
15 had gone home. Democrat Don Siegelman’s victory was handed to Republican Bob
16 Riley, and the recount Siegelman requested was denied. Six months after the election, the
17 vendor shrugged. “Something happened. I don’t have enough intelligence to say exactly
18 what,” said Mark Kelley of ES&S.

19 [...]

20 In the 2002 general election, a computer miscount overturned the House District
21 11 result in Wayne County, North Carolina. Incorrect programming caused machines to
22 skip several thousand partyline votes, both Republican and Democratic. Fixing the error
23 turned up 5,500 more votes and reversed the election for state representative.

24 [...]

25 Voting machines failed to tally “yes” votes on the 2002 school bond issue in
26 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

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

3 73. By 2004, explicit evidence that electronic voting machines were susceptible to
4 intentional manipulation, and that malicious actors sought to exploit this vulnerability, became
5 public. In that year, cyber expert Clint Curtis testified under oath before the House Judiciary
6 Committee that he had previously been hired to create a program that would change the results
7 of an election without leaving any trace of the change. He claimed he wrote this program with
8 ease. Mr. Curtis' testimony can be watched here:
9 <https://www.youtube.com/watch?v=JEzY2tnwExs>.
10
11

12 74. During the next election cycle, in 2006, a team of computer scientists at Princeton
13 University analyzed the Diebold AccuVote-TS voting machine, then one of the most widely-
14 deployed electronic voting platforms in the United States. They found, “Malicious software
15 running on a single voting machine can steal votes with little risk of detection. The malicious
16 software can modify all of the records, audit logs, and counters kept by the voting machine, so
17 that even careful forensic examination of these records will find nothing amiss. . . . Anyone who
18 has physical access to a voting machine, or to a memory card that will later be inserted into a
19 machine, can install said malicious software using a simple method that takes as little as one
20 minute. . . . AccuVote-TS machines are susceptible to voting machine viruses – computer
21 viruses that can spread malicious software automatically and invisibly from machine to machine
22 during normal pre- and post-election activity.” The Princeton team prepared a video
23 demonstration showing how malware could flip votes. In the video, mock election votes were
24
25
26

⁶ Available at <https://blackboxvoting.org/black-box-voting-book/>.

1 cast in favor of George Washington by a 4 to 1 margin, but the paper print-out that reported the
2 results showed Benedict Arnold prevailing by a margin of 3 to 2. Malicious vote-stealing
3 malware was the sole reason for reallocation of votes. The malware deleted itself after the
4 election, leaving no evidence that the voting machine was ever hijacked or any votes stolen.
5

6 75. In 2009 Diebold sold (at a loss) “Premier,” its electronic voting systems business
7 unit, which by then was known for its technical problems and unreliable security and accuracy.
8 The Premier intellectual property passed (from ES&S) to Dominion in May 2010. That
9 intellectual property included the GEMS election management system software. Dominion
10 quickly incorporated GEMS into its own products and by 2011 was selling election equipment
11 that had updated GEMS software at its heart. But GEMS was notorious for being, according to
12 Harper’s Magazine, “a vote rigger’s dream” that “could be hacked, remotely or on-site, using
13 any off-the-shelf version of Microsoft Access, and password protection was missing for
14 supervisor function.” Lack of encryption on its audit logs “allowed any trace of vote rigging to
15 be wiped from the record.” Computer scientists from Johns Hopkins University and Rice
16 University found GEMS “far below even the most minimal security standards applicable in
17 other contexts” and “unsuitable for use in a general election.”
18
19
20

21 76. In 2015 the Brennan Center for Justice issued a report listing two and a half-pages
22 of instances of issues with voting machines, including a 2014 investigation which found “voters
23 in Virginia Beach observed that when they selected one candidate, the machine would register
24
25
26

1 their selection for a different candidate.”⁷ The investigation also found that the Advanced Voting
2 Solutions WINVote machine, which is Wi-Fi-enabled, “had serious security vulnerabilities”
3 because wireless cards on the system could allow “an external party to access the [machine] and
4 modify the data [on the machine] without notice from a nearby location,” and “an attacker could
5 join the wireless ad-hoc network, record voting data or inject malicious [data.]”
6

7 77. In 2016, following in the footsteps of the Johns Hopkins, Rice, and 2006 Princeton
8 teams, Princeton Professor of Computer Science Andrew Appel told an interviewer how he had
9 purchased a voting machine for \$82 on the internet – the Sequoia AVC Advantage, still set to be
10 used in the 2016 election in a number of states – and replaced the machine’s ROM chips in mere
11 minutes using little more than a screwdriver, thereby “throw[ing] off the machine’s results,
12 subtly altering the tally of votes, never to betray a hint to the voter.”⁸
13
14
15
16
17
18
19
20
21
22

23
24 ⁷ Lawrence Norden and Christopher Famighetti, *America’s Voting Machines at Risk*, Brennan
25 Center for Justice, p.13 (Sep. 15, 2014) (available at <https://www.brennancenter.org/our-work/research-reports/americas-voting-machines-risk>).

26 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/>).



12 78. During that 2016 election cycle evidence emerged of foreign state actors seeking
13 to affect U.S. voting. “Russian agents probed voting systems in all 50 states, and successfully
14 breached the voter registration systems of Arizona and Illinois.”⁹ The Robert Mueller report and
15 an indictment of twelve Russian agents later confirmed that Russian hackers had targeted
16 vendors that provide election software, and Russian intelligence officers “targeted employees of
17 [REDACTED], a voting technology company that developed software used by numerous U.S.
18 counties to manage voter rolls, and installed malware on the company network.”¹⁰
19

20 79. After these revelations about the 2016 election, Jake Braun, a former security
21 advisor for the Obama administration and organizer of the DEFCON Hacking Conference was
22

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

26 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>).

1 asked in 2017, “Do you believe that right now, we are in a position where the 2020 election will
2 be hacked?” He answered, “Oh, without question. I mean the 2020 election will be hacked no
3 matter what we do.”
4

5 80. Following a 2017 runoff election in a Georgia congressional race, an advocacy
6 organization and individual voters filed suit in federal district court seeking to set aside the
7 results. They alleged the election “took place in an environment in which sophisticated hackers
8 – whether Russian or otherwise – had the capability and intent to manipulate elections in the
9 United States” and had “easy access” to do so.
10

11 81. The Georgia plaintiffs supported their allegations with expert testimony from
12 Logan Lamb, who testified that he freely accessed official Georgia state election files hosted on
13 an “elections.kennesaw.edu” server, including voter histories and personal information of all
14 Georgia voters; tabulation and memory card programming databases for past and future
15 elections; instructions and passwords for voting equipment administration; and executable
16 programs controlling essential election resources. Lamb stated that these sensitive files had been
17 publicly exposed for so long that Google had cached (i.e., saved digital backup copies of) and
18 published the pages containing many of them. Lamb said the publicly accessible files created
19 and maintained on this server were used to program virtually all other voting and tabulation
20 equipment used in Georgia’s elections.
21
22

23 82. Another piece of expert evidence in the Georgia litigation is a declaration from
24 Harri Hurst dated August 24, 2020 in which Hursti concludes that “the voting system is being
25 operated in Fulton County in a manner that escalates the security risk to an extreme level.”
26

1 Hursti based this conclusion in part on his observations that optical scanners would inexplicably
2 reject ballots; that the optical scanners would experience lengthy and unexplained scanning
3 delays; that the vendor, Dominion, failed to ensure a trained technician was on-site to address
4 problems with its equipment; that Dominion employees interfered with Hursti's efforts to
5 observe the upload of memory devices; that Dominion refused to cooperate with county
6 personnel; and that computers running Dominion software were vulnerable due to inadequate
7 "hardening" against a security attack.¹¹
8
9

10 83. The Georgia plaintiffs asked the court to enter a preliminary injunction barring
11 Georgia in the 2020 general election from using certain Dominion electronic voting machines.
12 On October 11, 2020, the federal court issued an order finding substantial evidence that the
13 system was plagued by security risks and the potential for votes to be improperly rejected or
14 misallocated. It wrote, "The Plaintiffs' national cybersecurity experts convincingly present
15 evidence that this is not a question of 'might this actually ever happen?' – but 'when it will
16 happen.'"
17

18 84. In 2019 a group of election security experts found "nearly three dozen backend
19 election systems in 10 states connected to the internet over the last year," including in "critical
20 swing states" Wisconsin, Michigan, and Florida. Some of the jurisdictions "were not aware that
21 their systems were online" and were "publicly saying that their systems were never connected to
22
23
24
25

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

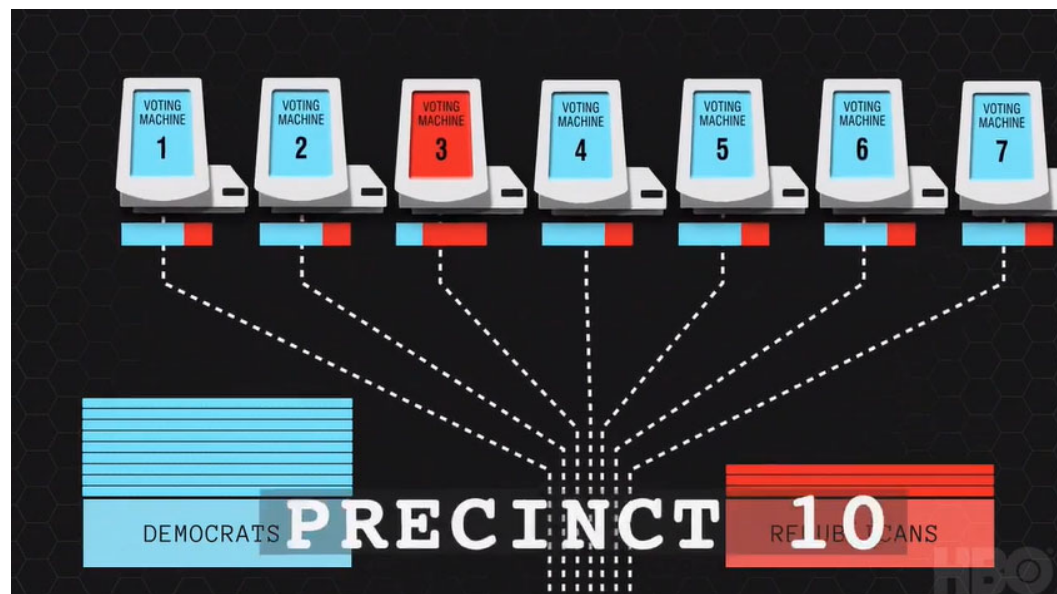
1 the internet because they didn't know differently."¹² The Associated Press reported that the vast
2 majority of 10,000 election jurisdictions nationwide were still using Windows 7 or older
3 operating systems to create ballots, program voting machines, tally votes, and report counts,
4 which was a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

8
9 85. In March 2020, the documentary *Kill Chain: The Cyber War on America's*
10 *Elections* detailed the vulnerability of electronic voting machines. In the film, Hursti showed
11 that he hacked digital election equipment to change votes back in 2005, and said the same
12 Dominion machine that he hacked in 2005 was slated for use in 20 states for the 2020 election.
13 *Kill Chain* also included facts about a Georgia election in which one machine out of seven in a
14 precinct registered a heavy majority of Republican votes, while every other machine in the
15 precinct registered a heavy majority of Democratic votes. Dr. Kellie Ottoboni, Department of
16 Statistics, UC Berkeley, stated the likelihood of this happening by chance was less than one in a
17 million.¹⁴

23 ¹² Kim Zetter, *Critical U.S. Election Systems Have Been Left Exposed Online Despite Official*
24 *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>).

25 ¹³ Tami Abdollah, *New election systems use vulnerable software*, Associated Press (July 13,
26 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>).

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

3
4 88. Leading electronic voting machine manufacturers source many parts from China,
5 Taiwan, and the Philippines.¹⁷

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

8 89. As the years passed and the evidence mounted, lawmakers and officials
9 throughout the nation have realized these problems with electronic voting machines cannot be
10 ignored.
11

12 90. The Congressional Task Force on Election Security issued a Final Report in
13 January 2018 that identified the vulnerability of U.S. elections to foreign interference:¹⁸
14 “According to DHS, Russian agents targeted election systems in at least 21 states, stealing
15 personal voter records and positioning themselves to carry out future attacks. . . media also
16 reported that the Russians accessed at least one U.S. voting software supplier . . . in most of the
17 targeted states officials saw only preparations for hacking . . . [but] in Arizona and Illinois, voter
18 registration databases were reportedly breached. . . If 2016 was all about preparation, what more
19
20

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

24 ¹⁷ Ben Popken, Cynthia McFadden and Kevin Monahan, *Chinese parts, hidden ownership,*
25 *growing scrutiny: Inside America's biggest maker of voting machines*, NBC News (Dec. 19,
26 2019) ([https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-
inside-america-s-biggest-n1104516](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>).

1 can they do and when will they strike? . . . [W]hen asked in March about the prospects for future
2 interference by Russia, then-FBI Director James Comey testified before Congress that:
3 ‘[T]hey’ll be back. They’ll be back in 2020. They may be back in 2018.’”¹⁹
4

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

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

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

19 • “trouble-plagued companies” responsible for manufacturing and
20 maintaining voting machines and other election administration equipment, “have long
21 skimmed on security in favor of convenience,” leaving voting systems across the country
22 “prone to security problems.”

23 • “the election technology industry has become highly concentrated ...
24 Today, three large vendors – Election Systems & Software, Dominion, and Hart
25 InterCivic – collectively provide voting machines and software that facilitate voting for
26 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.

1 falling apart, across the country, as vendors neglect to innovate and improve important
2 voting systems, putting our elections at avoidable and increased risk. . . . Moreover, even
3 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.’”

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

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

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

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

21 96. Senator Wyden stated in an interview, “[T]oday, you can have a voting machine
22 with an open connection to the internet, which is the equivalent of stashing American ballots in
23
24
25
26

1 the Kremlin. . . . [As] of today, what we see in terms of foreign interference in 2020 is going to
2 make 2016 look like small potatoes. This is a national security issue! . . . The total lack of
3 cybersecurity standards is especially troubling . . . But the lack of cybersecurity standards leads
4 local officials to unwittingly buy overpriced, insecure junk. Insecure junk guarantees three
5 things: a big payday for the election-tech companies, long lines on Election Day, and other
6 hostile foreign governments can influence the outcome of elections through hacks.”
7

8
9 97. In March of 2022, White House press secretary Jen Psaki said the Russian
10 government in 2016 “hacked our election here” in the United States.

11 98. The following month, Dara Lindenbaum, a nominee to serve on the Federal
12 Election Commission, testified before the Senate Rules and Administration Committee.
13 Lindenbaum was asked about her role as an election lawyer representing Stacey Abrams’s
14 campaign for governor of Georgia in 2018. Lindenbaum acknowledged she had alleged voting
15 machines were used to illegally switch votes from one candidate to another during the 2018
16 election in Georgia.²⁰
17

18
19 99. Dominion presented its Democracy Suite 5.5-A voting system to the State of
20 Texas for certification to be used in public elections in Texas. In January 2019, the State of
21 Texas rejected Dominion’s application and refused to certify Democracy Suite 5.5-A. On
22 October 2 and 3, 2019, Dominion presented Democracy Suite 5.5-A to the State of Texas for
23 examination a second time, seeking certification for use in public elections in Texas. Again,
24

25
26 _____
²⁰ PN1758 — Dara Lindenbaum — Federal Election Commission,
<https://www.congress.gov/nomination/117th-congress/1758>;
https://www.youtube.com/watch?v=wCPLL_D_spc

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

3
4 100. The experts designated by Texas to evaluate Democracy Suite 5.5-A flagged risk
5 from the system’s connectivity to the internet despite “vendor claims” that the system is
6 “protected by hardening of data and IP address features,” stating, “[T]he machines could be
7 vulnerable to a rogue operator on a machine if the election LAN is not confined to just the
8 machines used for the election . . . The ethernet port is active on the ICX BMD during an
9 election. . . . This is an unnecessary open port during the voting period and could be used as an
10 attack vector.” Other security vulnerabilities found by Texas include use of a “rack mounted
11 server” which “would typically be in a room other than a room used for the central count” and
12 would present a security risk “since it is out of sight.” In summary, “The examiner reports
13 identified multiple hardware and software issues Specifically, the examiner reports raise
14 concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose;
15 operates efficiently and accurately; and is safe from fraudulent or unauthorized manipulation.”
16
17

18
19 101. The Texas Attorney General explained, “We have not approved these voting
20 systems based on repeated software and hardware issues. It was determined they were not
21 accurate and that they failed — they had a vulnerability to fraud and unauthorized
22 manipulation.”

23
24 102. Dominion’s DVS 5.5-B voting system, set to be used in the Midterm Election in
25 Arizona, is substantially similar to the 5.5-A system that twice failed certification in Texas.
26

1 103. Though Texas did certify ES&S electronic voting machines for use in Texas,
2 ES&S voting systems are, like Dominion’s voting systems, opaque, easily hacked, and
3 vulnerable to incorporation of compromised components through ES&S’s supply chain.
4

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

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

10 105. John Poulous, the CEO of Dominion Voting Systems, testified in December 2020
11 that Dominion’s election systems are “closed systems that are not networked meaning they are
12 not connected to the internet.” This is false.
13

14 106. In a May 2016 interview, Dominion Vice President Goran Obradovic stated, “All
15 devices of the ImageCast series have additional options such as modems for wireless and wired
16 transfer of results from the very polling place....”²² During the 2020 election Dominion election
17 equipment was connected to the internet when it should not have been.²³ A Dominion
18 representative in Wayne County, Michigan stated that during the voting in the 2020 election
19
20
21

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

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

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

3
4 107. On Monday, November 2, 2020, the day before the 2020 election, Dominion
5 uploaded software updates into election equipment that Dominion had supplied in the United
6 States.²⁴ These software updates were unplanned and unannounced. In some counties in
7 Georgia, Dominion’s software update caused election equipment to malfunction the next day
8 during the election. The supervisor of one County Board of Elections stated that Dominion
9 “uploaded something last night, which is not normal, and it caused a glitch,” and “[t]hat is
10 something that they don’t ever do. I’ve never seen them update anything the day before the
11 election.” Dominion had earlier publicly denied that any updates just prior to election day were
12 made and that its election equipment was connected to the internet—both of which were false
13 statements.²⁵

14
15
16 108. In December 2020, the Department of Homeland Security’s Cybersecurity &
17 Infrastructure Agency (“CISA”) revealed that malicious hackers had compromised and exploited
18 SolarWinds Orion network management software products.²⁶ On April 15, 2021, the White
19

20
21
22
23 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>).

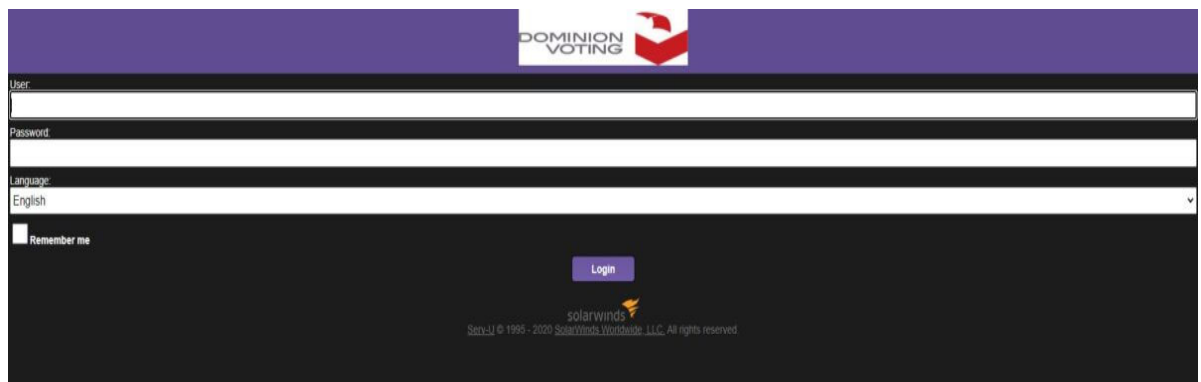
24 ²⁵ Isabel van Brugen, *Dominion Voting Machines Were Updated Before Election, Georgia
25 Official Confirms*, The Epoch Times (Dec. 4, 2020) (https://www.theepochtimes.com/dominion-voting-machines-were-updated-before-election-georgia-official-confirms_3604668.html).

26 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>).

1 House announced imposition of sanctions on Russia in response to Russian “malicious cyber
2 activities, such as the SolarWinds incident.”²⁷

3
4 109. Dominion CEO John Poulos stated that Dominion did not use SolarWinds.

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



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

17
18 112. No electronic voting system to be used in Arizona in the Midterm Election
19 employs “open source” technology, which is electronic equipment for which the details of the
20 components of the system, including its software, is published and publicly accessible. Though
21 Dominion and E&S do not offer open source voting technology, it has been available to
22 Defendants from other vendors for years.

23
24
25 ²⁷ The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian*
26 *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/>).

1 113. Defendants have failed or refused to institute open source voting technologies in
2 Arizona, even though such technology would promote both security and transparency, as voters
3 and office-seekers throughout Arizona would know the specific risks to, or manipulation of,
4 election results.
5

6 114. This lack of transparency by electronic voting machine companies has created a
7 “black box” system of voting which lacks credibility and integrity.
8

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

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

13 116. Dominion Democracy Suite software was used to tabulate votes in 62 Colorado
14 counties, including Mesa County and Elbert County, during the 2020 election. Subsequent
15 examination of equipment from Mesa County and Elbert County showed the Democracy Suite
16 software created unauthorized databases on the hard drive of the election management system
17 servers. On March 21, 2022, electronic database expert Jeffrey O’Donnell and computer science
18 expert Dr. Walter Daugherty published a report concluding that ballots were manipulated in the
19 unauthorized databases on the Mesa County server during Colorado’s November 2020 and April
20 2021 elections.
21

22 117. On February 28, 2022, and after a comprehensive review of the Dominion systems
23 used in Colorado, cybersecurity expert Douglas Gould published a report concluding that the
24 system was “configured to automatically overwrite log files that exceed 20 MB, thereby
25
26

1 violating federal standards that require the preservation of log files,” that it was configured “to
2 allow any IP address in the world to access the SQL service port, (1433), which violates 2002
3 VSS security standards,” and that it “uses generic user IDs and passwords and a common shared
4 password, some of which have administrative access,” in violation of 2002 VSS security
5 standards.
6

7 118. Electronic forensic experts examined equipment used in Michigan to administer
8 voting during the 2020 election and concluded the equipment had been connected to the internet,
9 either by Wi-Fi or a LAN wire, that there were multiple ways the election results could have
10 been modified without leaving a trace; and the same problems have been around for 10 years or
11 more. One expert “examined the forensic image of a Dominion ICX system utilized in the
12 November 2020 election and discovered evidence of internet communications to a number of
13 public and private IP addresses.”
14
15

16 119. In Wisconsin, during the voting in the 2020 election, Dominion election
17 equipment that was not supposed to be connected to the internet was connected to a “hidden”
18 Wi-Fi network.²⁸
19

20 120. In April 2021, the Biden administration announced sanctions against Russia for
21 election interference and hacking in the 2020 United States presidential election.²⁹
22
23

24 ²⁸ M.D. Kittle, *Emails: Green Bay’s ‘Hidden’ Election Networks*, Wisconsin Spotlight (Mar. 21,
25 2021) (<https://wisconsinspotlight.com/emails-green-bays-hidden-election-networks/>).

26 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>).

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

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

11 123. Retired Wisconsin Supreme Court Justice Michael Gableman conducted an
12 investigation of the 2020 election in Wisconsin at the direction of the Wisconsin Assembly.
13 Gableman issued a report in March 2022 noting that “at least some machines had access to the
14 internet on election night.”³¹ He concluded that several machines manufactured by ES&S and
15 used in the 2020 election in Wisconsin were “made with a 4G wireless modem installed,
16 enabling them to connect to the internet through a Wi-Fi hotspot.”
17
18
19
20
21
22
23
24

25 ³⁰ *Maricopa County Forensic Election Audit, Volume I*, pp.1-3 (Sept. 24, 2021) (available at
26 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.

1 124. During a December 30, 2020 live-streamed hearing held by the Georgia Senate
2 Judiciary Subcommittee on Elections, an expert witness testified that an active Dominion
3 polling pad had been hacked and the intrusion was being maintained even as he was speaking.³²
4

5 **G. Arizona’s Voting Systems Do Not Comply with State or Federal Standards**
6

7 125. All voting systems and voting equipment used in Arizona must comply with
8 standards set forth in Federal Election Commission Publication “2002 Voting Systems
9 Standards” (“2002 VSS”). A.R.S. § 16-442(B).
10

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

12 g. Record and report the date and time of normal and abnormal events;

13 h. Maintain a permanent record of all original audit data that cannot be
14 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.)

15 i. Detect and record every event, including the occurrence of an error
16 condition that the system cannot overcome, and time-dependent or programmed
17 events that occur without the intervention of the voter or a polling place operator;

18 [VSS, § 2.2.4.1]

19 ...

20 a. Maintain the integrity of voting and audit data during an election, and for
21 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

22 b. Protect against the failure of any data input or storage device at a location
23 controlled by the jurisdiction or its contractors, and against any attempt at
improper data entry or retrieval.

24 [VSS, § 4.3]
25

26

³² Hearing of Georgia Senate Judiciary Subcommittee on Elections, Dec. 30, 2020
(<https://www.youtube.com/watch?v=D5c034r0RIU> beginning at 4:07:58).

1 127. Defendant Hobbs has statutory duties to test, certify, and qualify software and
2 hardware that is used on county election systems. A.R.S. § 16-442(B). Defendant Hobbs
3 certified Dominion’s DVS 5.5-B voting system for use in Arizona on or around November 5,
4 2019. The DVS 5.5-B system includes the Dominion ImageCast Present2 (“ICP2”).

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

16 129. University of Michigan Professor of Computer Science and Engineering J. Alex
17 Halderman performed a thorough examination of voting equipment used in Georgia, which is
18 also used in Arizona. In a series of expert reports submitted in litigation still pending in the
19 Northern District of Georgia, Professor Halderman stated that this voting equipment can be
20 manipulated “to steal votes,” has “numerous security vulnerabilities” that “would allow
21 attackers to install malicious software” through either “temporary physical access (such as that
22 of voters in the polling place) or remotely from election management systems.” He stated that
23 these “are not general weaknesses or theoretical problems, but rather specific flaws” which he
24 was “prepared to demonstrate proof-of-concept malware that can exploit them to steal votes.”
26

1 He also concluded that the equipment “is very likely to contain other, equally critical flaws that
2 are yet to be discovered.” He specifically noted that this same equipment, the ICX, will be used
3 in 2022 in “for accessible voting in Alaska and large parts of Arizona . . .”
4

5 130. In the Midterm Election, Arizona intends to use, in part, the same software about
6 which Dr. Halderman testified. The ICX fails to meet VSS standards for the reasons stated in
7 Dr. Halderman’s reports.
8

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

11 132. By seeking to use DVS 5.5-B in the Midterm Election, Defendant intends to
12 facilitate violations of Arizona law and federal law.
13

14 133. By choosing to continue using the non-compliant system in the Midterm Election
15 without taking any meaningful steps to remedy known security breaches affecting Arizona
16 voters, Defendants know that they will cause voters to cast votes in Midterm Election on an
17 inaccurate, vulnerable and unreliable voting system that cannot produce verifiable results and
18 does not pass constitutional or statutory muster.
19

20 **H. Arizona’s Audit Regime is Insufficient to Negate Electronic Voting Machines’**
21 **Vulnerabilities**

22 134. Post-election audits do not and cannot remediate the security problems inherent in
23 the use of electronic voting machines.
24

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

1 136. Dr. Halderman stated in a Declaration dated August 2, 2021, that malware can
2 defeat “all the procedural protections practiced by [Georgia], including acceptance testing, hash
3 validation, logic and accuracy testing, external firmware validation, and risk-limiting audits
4 (RLAs).” Dr. Halderman testified that the voting system at issue in Georgia is used in fifteen
5 other states, including Arizona.
6

7 137. Electronic voting systems vendors have repeatedly refused to comply with post-
8 election audits, diminishing the audits’ ability to yield reliable conclusions about the validity of
9 the election results.
10

11 138. On July 26, 2021, Arizona Senate leaders issued subpoenas to Dominion Voting
12 Systems in connection with the Senate’s audit of the 2020 election in Maricopa County,
13 Arizona. Among other materials, the July 26 subpoenas sought production of usernames,
14 passwords, tokens, and pins to the ballot tabulation machines the Maricopa County rents from
15 Dominion, including all that would provide administrative access.
16

17 139. Dominion flatly refused to comply with this validly-issued legislative subpoena.
18 In a letter to Senate President Karen Fann, Dominion wrongly claimed the subpoena seeking
19 credentials necessary to access the Dominion voting systems to validate an election “violat[ed]
20 [Dominion’s] constitutional rights and ... exceed[ed] the Legislature’s constitutional and
21 statutory authority” and that responding to the subpoena would “cause grave harm” to
22 Dominion.
23
24

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

1 it “is under no obligation to respond,” despite the fact the subpoena was issued by the state
2 Senate.

3
4 141. Any voting system that relies on the hidden workings of electronic devices in the
5 casting and/or counting of the vote is a system of which voters may reasonably be suspicious.
6 Post-election audits are not sufficient to alleviate their reasonable suspicions because voting
7 machine manufacturers have demonstrated that they will not provide the information necessary
8 to audit an election.
9

10 142. To restore legitimacy to Arizona’s election regime for all voters, regardless of
11 party, and to comply with constitutional and legal requirements, a secure and feasible alternative
12 must supplant reliance on faulty electronic voting systems.
13

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

16 143. Plaintiffs seek for the Court to Order, an election conducted by paper ballot, as an
17 alternative to the current framework. To satisfy constitutional requirements of reliability,
18 accuracy, and security, the following is a summary of procedures that should be implemented:
19

20 • Ballots are cast by voters filling out paper ballots, by hand. The ballots are then
21 placed in a sealed ballot box. Each ballot bears a discrete, unique identification number, which is
22 made known by election officials only to the voter, so that the voter can later verify whether his
23 or her ballot was counted properly. All ballots will be printed on specialized paper to confirm
24 their authenticity.
25
26

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

3
4 • With party representatives, ballot boxes are unsealed, one at a time, and ballots are
5 removed and counted in batches of 100, then returned to the ballot box. When all ballots in a
6 ballot box have been counted, the box is resealed, with a copy of the batch tally sheets left inside
7 the box, and the batch tally sheets carried to the tally center with a uniform chain of custody.

8
9 • Ballots are counted, one at a time, by three independent counters, who each
10 produce a tally sheet that is compared to the other tally sheets at the completion of each batch.

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

13
14 • Vote counting from paper ballots is conducted in full view of multiple, recording,
15 streaming cameras that ensure a) no ballot is ever touched or accessible to anyone off-camera or
16 removed from view between acceptance of a cast ballot and completion of counting, b) all
17 ballots, while being counted are in full view of a camera and are readable on the video, and c)
18 batch tally sheets and precinct tally sheets are in full view of a camera while being filled out and
19 are readable on the video.

20
21 • Each cast ballot, from the time of receipt by a sworn official from a verified,
22 eligible elector, remains on video through the completion of precinct counting and reporting.

23
24 • The video be live-streamed for public access and archived for use as an auditable
25 record, with public access to replay a copy of that auditable record.

26

1 • Anonymity will be maintained however, any elector will be able to identify their
2 own ballot by the discrete, serial ballot number known only to themselves, and to see that their
3 own ballot is accurately counted
4

5 144. Every county in Arizona, regardless of size, demographics, or any other ostensibly
6 unique characteristic, can simply and securely count votes cast on paper ballots without using
7 centralized machine-counting or computerized optical scanners.
8

9 145. The recent hand count in Maricopa County, the second largest voting jurisdiction
10 in the United States, offers Defendant Hobbs a proof-of-concept and a superior alternative to
11 relying on corruptible electronic voting systems. Voting jurisdictions larger than any within
12 Arizona, including France and Taiwan, have also proven that hand-count voting can deliver
13 swift, secure, and accurate election results.
14

15 **J. Past and Threatened Conduct of Defendant Hobbs**
16

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

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

23 A.R.S. § 16-452 (A).

24 • “The secretary of state shall provide personnel who are experts in electronic voting
25 systems and procedures and in electronic voting system security to field check and review
26 electronic voting systems and recommend needed statutory and procedural changes.”

 A.R.S. § 16-452 (D).

1
2 147. Defendant Hobbs, in her capacity as Secretary of State, is further charged with
3 ensuring that electronic voting systems used throughout Arizona meet the following
4 requirements:

5 • “Be suitably designed for the purpose used and be of durable construction, and
6 may be used safely, efficiently and accurately in the conduct of elections and counting
7 ballots...”

8 • “When properly operated, record correctly and count accurately every vote
9 cast...” and

10 • “Provide a durable paper document that visually indicates the voter's selections,
11 that the voter may use to verify the voter's choices, that may be spoiled by the voter if it fails to
12 reflect the voter's choices and that permits the voter to cast a new ballot.”

13 A.R.S. § 16-446 (B).

14 148. Defendant Hobbs, in her capacity as Secretary of State, is further charged with
15 ensuring that all computer election programs filed with the office of the Secretary of State shall
16 be used by the Secretary of State or Attorney General to preclude fraud or any unlawful act.

17 A.R.S. § 16-445(D).

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

20 150. Defendant Hobbs, acting in her official capacity as the Secretary of State, has
21 shown her intention to require the use of electronic voting systems for all Arizona voters in the
22 Midterm Election.
23

24 151. In so doing, Defendant Hobbs will violate her duties under A.R.S. § 16-442(B),
25 and violate the Constitutional rights of Plaintiffs and all voters in the State of Arizona.
26

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

2
3 152. The Maricopa Defendants and Pima Defendants, acting in their official capacity,
4 are charged with the duty to:

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

11 A.R.S. § 11-251.

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

17
18 154. The Maricopa Defendants and Pima Defendants have, in the past, failed in the
19 duties set forth above by failing to, among other things, ensure that:

- 20 • operating systems and antivirus definitions of electronic voting systems were
21 properly updated;
22
23 • electronic election files and security logs were preserved;
24 • election management servers were not connected to the Internet;
25 • access to election equipment was limited to authorized personnel; and
26 • communications over the system network were properly monitored.

1 155. The Maricopa Defendants and Pima Defendants intend to rely on the use of
2 deficient electronic voting systems in the Midterm Election.
3

4 **L. Imminent Injury**

5 156. Plaintiff Lake seeks the office of Governor of the State of Arizona.
6

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

9 158. Plaintiff Lake intends to vote in the Midterm Election in Arizona. To do so, she
10 will be required to cast her vote, and have her vote counted, through electronic voting systems.
11

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

13 160. To gain that office, Plaintiff Finchem must prevail in the Midterm Election, in
14 which all votes will be tabulated, and many votes will be cast, on electronic voting systems.
15

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

18 162. All persons who vote in the Midterm Election, if required to vote using an
19 electronic voting system or have their vote counted using an electronic voting system, will be
20 irreparably harmed because the voting system does not reliably provide trustworthy and
21 verifiable election results. The voting system therefore burdens and infringes their fundamental
22 right to vote and have their vote accurately counted in conjunction with the accurate counting of
23 all other legal votes, and *only* other legal votes.
24
25
26

1 163. Any voter who votes using a paper ballot will be irreparably harmed in the
2 exercise of the fundamental right to vote if his or her vote is tabulated together with the votes of
3 other voters who cast ballots using an unreliable, untrustworthy electronic system.
4

5 164. Any voter will be irreparably harmed in the exercise of the constitutional,
6 fundamental right to vote if he or she is required to cast a ballot using – or in an election in
7 which anyone will use – an electronic voting system, or if his or her ballot is tabulated using an
8 electronic voting system.
9

10 165. Each of the foregoing harms to Plaintiff is imminent for standing purposes because
11 the Midterm Election is set to occur on a fixed date not later than eight months after the date
12 when this action is to be filed.
13

14 166. No Plaintiff can be adequately compensated for these harms in an action at law for
15 money damages brought after the fact because the violation of constitutional rights is an
16 irreparable injury.
17

18 **IV. CLAIMS**

19 **COUNT I: VIOLATION OF DUE PROCESS**

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

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

22 168. The right to vote is a fundamental right protected by the Due Process Clause of the
23 Fourteenth Amendment of the U.S. Constitution and Article 2, Section 4 of the Arizona
24 Constitution.
25
26

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

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

7 (a) Failed to provide reasonable and adequate protection against the real and substantial
8 threat of electronic and other intrusion and manipulation by individuals and entities
9 without authorization to do so;
10

11 (b) Failed to include the minimal and legally required steps to ensure that such equipment
12 could not be operated without authorization; to provide the minimal and legally required
13 protection for such equipment to secure against unauthorized tampering; to test, inspect,
14 and seal, as required by law, the equipment to ensure that each unit would count all votes
15 cast and that no votes that were not properly cast would not be counted; and to ensure
16 that all such equipment, firmware, and software is reliable, accurate, and capable of
17 secure operation as required by law;
18

19 (c) Failed to provide a reasonable and adequate method for voting by which Arizona
20 electors' votes would be accurately counted.
21

22 171. By choosing to move forward in using an unsecure system, Defendants willfully
23 and negligently abrogated their statutory duties and abused their discretion, subjecting voters to
24 cast votes on an illegal and unreliable system--a system that must be presumed to be
25 compromised and incapable of producing verifiable results.
26

1 172. Despite Defendants' knowledge that electronic voting systems used in Arizona do
2 not comply and cannot be made to comply with state and federal law, Defendants plan to
3 continue to use these non-compliant systems in the Midterm Election.
4

5 173. Plaintiffs ask this Court to declare that these Defendants violated the Due Process
6 Clause of the Fourteenth Amendment of the United States Constitution and Article 2, Section 4
7 of the Arizona Constitution; enjoin Defendants' use of electronic voting systems for future
8 elections; and award attorneys' fees and costs for Defendants' causation of concrete injury to
9 Plaintiffs, whose fundamental right to have their vote counted as cast was thwarted.
10

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

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

14 175. By requiring Plaintiffs to vote using electronic voting systems in the Midterm
15 Election which are unsecure and vulnerable to manipulation and intrusion there will be an
16 unequal voting tabulation of votes treating Plaintiffs who vote in Arizona differently than other,
17 similarly situated voters who cast ballots in the same election.
18

19 176. These severe burdens and infringements that Defendants will impose unequally on
20 Plaintiffs who vote through an electronic voting system will violate the Equal Protection Clause
21 of the Fourteenth Amendment.
22

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

1 178. Requiring voters to be deprived of their constitutional right to equal protection of
2 the laws as a condition of being able to enjoy the benefits and conveniences of voting in person
3 at the polls violates the unconstitutional conditions doctrine.
4

5 179. Unless Defendants are enjoined by this Court, then Plaintiffs will have no
6 adequate legal, administrative, or other remedy by which to prevent or minimize the irreparable,
7 imminent injury that is threatened by Defendants intended conduct. Accordingly, injunctive
8 relief against these Defendants is warranted.
9

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

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

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

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

17 183. Defendants have violated Plaintiffs' fundamental right to vote by deploying an
18 electronic voting equipment system that has:
19

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

23 (b) Failed to include the minimal and legally required steps to ensure that such equipment
24 could not be operated without authorization; to provide the minimal and legally required
25 protection for such equipment to secure against unauthorized tampering; to test, inspect,
26

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

5
6 (c) Failed to provide a reasonable and adequate method for voting by which Arizona
7 electors' votes would be accurately counted.

8
9 184. By choosing to move forward in using the non-compliant system, Defendants have
10 abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an
11 illegal and unreliable system--a system that is unsecure and vulnerable to manipulation and
12 intrusion and incapable of producing verifiable results.

13
14 185. Defendants' violation of the Due Process Clause is patently and fundamentally
15 unfair and therefore relief is warranted. Accordingly, Plaintiffs ask this Court to declare that
16 these Defendants violated the Due Process Clause of the Fourteenth Amendment of the United
17 States Constitution and Article 2, Section 4 of the Arizona Constitution; enjoin Defendants' use
18 of electronic voting systems for future elections; and award attorneys' fees and costs for
19 Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their
20 vote counted as cast was thwarted.

21
22 **COUNT IV: CIVIL ACTION FOR DEPRIVATION OF RIGHTS**
23 **UNDER 42 U.S.C. § 1983**

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

25 186. Plaintiffs incorporate and reallege all paragraphs in this Complaint.
26

1 187. The foregoing violations will occur as a consequence of Defendants acting under
2 color of state law. Accordingly, Plaintiffs bring this cause of action for prospective equitable
3 relief against Defendants pursuant to 42 U.S.C. § 1983.
4

5 188. By requiring the citizens of Arizona to vote using a system which may miscount
6 their votes, the Defendants will violate the rights of the citizens' under the Constitution of the
7 United States.
8

9 189. Unless Defendants are enjoined by this Court, then Plaintiffs will have no
10 adequate legal, administrative, or other remedy by which to prevent or minimize the irreparable,
11 imminent injury that is threatened by Defendants' intended conduct. Accordingly, appropriate
12 damages and injunctive relief against these Defendants is warranted.
13

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

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

17 191. Maricopa Defendants and Pima Defendants, as members of the Maricopa Board
18 and the Pima Board, are charged with statutory duties to electors in Arizona, including
19 Plaintiffs, under A.R.S. § 11-251.
20

21 192. Maricopa Defendants and Pima Defendants have failed to meet the duties set forth
22 in A.R.S. § 11-251 to adopt provisions necessary to preserve the health of Maricopa County and
23 Pima County.
24

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

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

3
4 194. Maricopa Defendants and Pima Defendants intend to continue in their failure to
5 meet these duties through the Midterm Election.

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

8
9 196. Unless Maricopa Defendants and Pima Defendants are enjoined by this Court, then
10 Plaintiffs will have not adequate administrative, or other remedy by which to prevent or
11 minimize the irreparable, imminent injury that is threatened by the intended conduct of
12 Maricopa Defendants and Pima Defendants. Accordingly, injunctive relief against these
13 Defendants is warranted.

14
15 **COUNT VI: DECLARATORY JUDGMENT - 28 U.S. CODE § 2201**
16 *(Against All Defendants)*

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

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

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

23
24 200. If the State of Arizona is allowed to proceed with an election as described above, it
25 will violate the rights of the citizens of the State by conducting an election with an unsecure,
26 vulnerable electronic voting system which is susceptible to manipulation and intrusion.

1 201. Because of the above-described issues regarding the election system to be used by
 2 Defendants, the Court should issue an Order enjoining the State from using any electronic
 3 voting system unless and until the system is made open to the public and subjected to scientific
 4 analysis to determine whether it is absolutely secure from manipulation or intrusion.
 5

6 **PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiffs respectfully request that this Court:
 8

- 9 1. Enter a judgment finding and declaring it unconstitutional for any public election
 10 to be conducted using any model of electronic voting system to cast or tabulate votes.
 11
- 12 2. Enter a preliminary and permanent injunction prohibiting Defendants from
 13 requiring or permitting voters to have votes cast or tabulated using any electronic voting system.
 14
- 15 3. Enter an Order directing Defendants to conduct the Midterm Election consistent
 16 with the summary of procedures set forth in paragraph 140 of this Complaint.
 17
- 18 4. Retain jurisdiction to ensure Defendants’ ongoing compliance with the foregoing
 Orders.
 19
- 20 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.
 21
- 22 6. Damages suffered by Plaintiffs to be determined at trial.
 23
- 24 7. Grant Plaintiff such other relief as the Court deems just and proper.
 25
 26

1 **DEMAND FOR JURY TRIAL**

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

3 DATED: April 22, 2022.

4 **PARKER DANIELS KIBORT LLC**

5 By /s/ Andrew D. Parker
6 Andrew D. Parker (AZ Bar No. 028314)
7 888 Colwell Building
8 123 N. Third Street
9 Minneapolis, MN 55401
10 Telephone: (612) 355-4100
11 Facsimile: (612) 355-4101
12 parker@parkerdk.com

13 **OLSEN LAW, P.C.**

14 By /s/ Kurt Olsen
15 Kurt Olsen (D.C. Bar No. 445279)*
16 1250 Connecticut Ave., NW, Suite 700
17 Washington, DC 20036
18 Telephone: (202) 408-7025
19 ko@olsenlawpc.com

20 * To be admitted *Pro Hac Vice*

21 *Counsel for Plaintiffs Kari Lake*
22 *and Mark Finchem*

23 **ALAN DERSHOWITZ CONSULTING LLC**

24 By /s/ Alan M. Dershowitz
25 Alan M. Dershowitz (MA Bar No. 121200)*
26 2255 Glades Road
Suite 321A
Boca Raton, FL 33431

* To be admitted *Pro Hac Vice*

Of Counsel for Plaintiffs Kari Lake
and Mark Finchem