[Proposed Plaintiffs' Preliminary Injunction, Doc. No. 33. (Jun. 08, 2022). Lake et al v.-Hobbs et al (no electronic voting machines in AZ Nov 2022 elections), Case No. 2:22-cv-00677-JJT (Judge John J. Tuchi), filed Apr. 22, 2022. (D. Ariz. 2022). Pacer.gov.]

PARKER DANIELS KIBORT
Andrew Parker (028314)
888 Colwell Building
123 Third Street North
Minneapolis, Minnesota 55401
parker@parkerdk.com
Telephone: (612) 355-4100
Facsimile: (612) 355-4101

OLSEN LAW, P.C.
Kurt Olsen (D.C. Bar No. 445279)*
1250 Connecticut Ave., NW, Suite 700
Washington, DC 20036
Telephone: (202) 408-7025
ko@olsenlawpc.com
* Admitted *Pro Hac Vice*

Alan M. Dershowitz (MA Bar No. 121200)#
1575 Massachusetts Avenue
Cambridge, MA 02138
To be admitted *Pro Hac Vice*

Attorneys for Plaintiffs

[https://en.wikipedia.org/wiki/John_Joseph_Tuchi]

[https://www.judiciary.senate.gov/imo/media/doc/Tuchi-Senate-Questionnaire-Final.pdf]

[https://www.judiciary.senate.gov/imo/media/doc/012814QFRs-Tuchi.pdf]

[https://ballotpedia.org/John_Tuchi]

[https://www.govinfo.gov/content/pkg/CHRG-113shrg24284/html/CHRG-113shrg24284.htm]

[Notes:

1987-1989: Hughes Aircraft Company, Missile Systems Division (now **Raytheon Corporation**)

1989-1991: **Andersen Consulting** (now Accenture)

1999-present: 5.5% shareholder in **Nueve Ltd.**

https://opencorporates.com/companies/us_wv/80493]

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Kari Lake; Mark Finchem, Plaintiffs, v. Kathleen Hobbs, as Arizona Secretary of State; Bill Gates; Clint Hickman; Jack Sellers; Thomas Galvin; and Steve Gallardo, in their capacity as members of the Maricopa County Board of Supervisors; Rex Scott; Matt Heinz; Sharon Bronson; Steve Christy; Adelita Grijalva, in their capacity as members of the Pima County Board of Supervisors, Defendants.	No. 22-cv-00677-DMF (Honorable John J. Tuchi) **PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION AND MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION** **Oral Argument Requested** Declaration of Benjamin R. Cotton, Declaration of Walter C. Daugherity, Declaration of Douglas Logan, Declaration of John R. Mills, Declaration of Shawn A. Smith, and Declaration of Andrew Parker filed in support.

PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

Pursuant to Rule 65(a) of the Federal Rules of Civil Procedure and to Rule 7.2 of the Rules of Practice and Procedure of the U.S. District Court for the District of Arizona, Plaintiffs hereby move the Court to enter a preliminary injunction barring Defendants from using computerized equipment to administer the collection, storage, counting, and tabulation of votes in any election until such time that the propriety of a permanent injunction is determined. This motion is based on Plaintiff's memorandum of law and the Declarations of Benjamin R. Cotton, Walter C. Daugherity, Douglas Logan, John R. Mills, Shawn A. Smith, and Andrew Parker, which are filed herewith.

MEMORANDUM OF POINTS AND AUTHORITIES

The right to vote and know that one's vote is fairly and accurately counted is foundational to our democracy. With this case Plaintiffs seek to eliminate the black box voting system that has developed in this country as it is used in this State. Arizona voters no longer know whether their vote has been accurately tabulated or manipulated. And there can be no spot check within reasonable levels of confidence. This is a violation of Plaintiffs' Constitutional rights.

For centuries, American voters recorded their votes by hand on paper ballots that were counted by human beings. In the last two decades, states including Arizona have adopted electronic, computerized voting systems. Expert analyses, studies and investigations have determined that even the most sophisticated computers can be and have been hacked. It is now widely accepted that the equipment used is often assembled or made in countries like China that allows unauthorized access. Indeed, countries like Russia, China, and Iran have thousands of highly trained individuals whose sole function is to penetrate commercial and government computers in the United States—including our election systems. In response, countries like France ban the use of computerized voting machines because of their inherent security flaws and opaqueness.

Experience has now shown the move to computerized voting in Arizona was a mistake – an unnecessary, unsecure change that opened election results to manipulation by unauthorized persons. This is not a partisan issue. Experts across the political spectrum have long sounded the alarm about the inherent insecurity and lack of transparency in computerized voting systems such as those used in Arizona. It is time to reverse this mistake. The right to vote is constitutionally guaranteed. Computerized voting systems leave an open door for votes to be changed, deleted, or fabricated in violation of constitutional requirements. A return to the tried-and-true paper ballots of the past – and of the present, in countries like France, Taiwan, and Israel – is necessary.

Plaintiffs submit this memorandum and related expert declarations and documentary evidence, and further request that the Court hear live testimony, in support of their request that this Court enter a preliminary injunction barring Defendants from using computerized equipment to administer the collection, storage, counting, and tabulation of votes in any election until such time that the propriety of a permanent injunction is determined. Computerized equipment is vulnerable to manipulation by unauthorized persons, meaning that the true results of an election that relies upon computerized equipment can never be known and Plaintiffs' constitutional rights to vote will be denied, if computerized equipment is used.

I.

FACTS

A. <u>2022 Election Upcoming</u>.

On November 8, 2022, Arizona will hold a statewide general election ("2022 Election") in which the holders of numerous public offices will be determined by majority vote, including the Arizona Governor and the Arizona Secretary of State. *See* A.R.S. § 16-

211. Administration of the 2022 Election requires Arizona, and counties within the State, to provide eligible Arizona voters with ballots and an opportunity to complete the ballots in secrecy and privacy; to collect the completed ballots; to count the number of legal votes for each candidate; and to tabulate across all precincts and counties the total number of votes each candidate received. *See* A.R.S. §§ 16-404, 405, 447, 450, 503, 517, 564, 602, 608, 609, 614, 615, 622, 646, 647. Arizona and Arizona counties intend to use computerized devices ("Electronic Voting Systems") to complete these administrative tasks. Ariz. Sec'y of State, *2022 Election Cycle/Voting Equipment* (Feb. 2022 Revision). Decl. of Andrew Parker ¶ 2 & Ex. A ("Parker Decl.").[1] However, the Electronic Voting Systems provide a means for unauthorized persons to manipulate the reported vote counts in the election and thereby change the candidate who is deemed the winner.

- Defendant Hobbs has approved, and Maricopa County intends to use, the ImageCast X BMD, the ICC Canon DR-G1130, and the Democracy Suite 5.5b Election Management System (EMS) software running on a computer server, in a computerized system supplied by Dominion Voting Systems. Parker Decl. ¶¶ 2-3 & Exs. A & B; *see also* Parker Decl. ¶ 4 & Ex. C (Test Report). ImageCast X BMD is a ballot-marking device – a touchscreen computer used to electronically complete a ballot which is then printed by an attached printer. *See* Parker Decl. ¶ 4 & Ex. C at 3-4. The ICC Canon DR-G1130 is a scanner used for scanning and counting ballots. *Id*. at 3, 12. Democracy Suite 5.5b EMS is a set of software applications intended to be used to manage elections, including election results acquisition, validation, tabulation, reporting, and publishing, and holding election data. *Id*. at 1-2.

[1] *Available at* https://azsos.gov/sites/default/files/2022_Election_Cycle_Voting_Equipment-Feb-Final.pdf.

- Defendant Hobbs has approved, and Pima County intends to use, the ExpressVote (BMD), the DS850, and the ElectionWare 6.0.4.0 Election Management System software, in a system supplied by Election Systems & Software, LLC ("ES&S"). Parker Decl. ¶¶ 2-3 & Exs. A & B. ExpressVote is a ballot-marking device – a touchscreen computer used to electronically complete a ballot which is then printed. *See* Parker Decl. ¶ 5 & Ex. D at 7. The DS850 is a scanner used for converting marks on paper ballots to electronic Cast Vote Records. *Id*. at 8. ElectionWare EMS is a software application used to manage elections, including ballot formation, equipment configuration, result consolidation, adjudication, and report creation. *Id*. at 7.
- Defendant Hobbs has approved, and at least one county in Arizona intends to use, the OpenElect 2.1 FVT, the OpenElect 2.8 OVCS, and the OCS OpenElect 2.1, in a system supplied by Unisyn Voting Solutions. Parker Decl. ¶¶ 2-3 & Exs. A & B. The OpenElect FVT is a ballot-marking device – a device used to electronically complete a ballot which is then printed. Parker Decl. ¶ 6 & Ex. E at 5. The OpenElect OVCS is a bulk scanner and computer that reads ballots and permits evaluation of ballots with questionable marks and "chang[ing] votes in accordance to the voter's perceived intent." *Id*. at 1, 2, 6-7. OCS OpenElect is an election management system (EMS) that includes applications to receive and validate voting data, retrieve vote files and ballot images, evaluate ballots with questionable marks and "change votes in accordance to the voter's perceived intent," store results from precincts, and generate tabulator reports. *Id*. at 1-2.

The Dominion, ES&S, and Unisyn systems are all Electronic Voting Systems. The BMDs they use, the ballot scanners and tabulators they use, and the computer servers running EMS software they use, are all computerized, electronic devices.

B. Electronic Voting Systems Not Reliable.

Since 2002, mounting evidence and experience has shown Electronic Voting Systems to be unreliable, unsecure, and vulnerable to undetected manipulation of the voting results they report. Indeed, just last week, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") issued a public statement concerning a Dominion voting system used in sixteen states, including Arizona. The statement detailed a number of critical vulnerabilities discovered by a computer scientist in connection with litigation to prohibit the use of the electronic voting machines used in Georgia.[2]

1. Electronic Devices

The vulnerability of Electronic Voting Systems results from basic principles of the behavior of electronic devices. In broad terms, "electronic voting machines," "electronic voting systems," and "electronic election equipment" refer to any computerized devices or equipment used to cast, print, count, tabulate, process, and/or store ballot images or election results. Decl. of Douglas Logan ¶ 15 ("Logan Decl."). "Source code" or generically "code" refers to instructions written in a programming language that tells a computerized device, such as an electronic voting machine, how to operate, "think," and process data. *Id.* ¶ 16. "Erroneous code" is source code that, when run as a computer

[2] *Curling et al. v. Raffensperger et al.*, No. 1:17-CV-2989-AT, ECF 1391 (N.D. Ga. June 4, 2022). CISA's statement is available at https://www.cisa.gov/uscert/ics/advisories/icsa-22-154-01.

program, does not perform the expected behavior and intention of the program. *Id.* ¶ 19. Erroneous code may be caused by a "bug" (an unintentional error by a programmer) or "malicious code" (an intentional cause of adverse behavior by the computerized device). *Id.* ¶¶ 19-21. A "malicious program" is a computer program that is created or otherwise contains "malicious code," and therefore performs some adverse behavior. *Id.* ¶ 22.

A person who gains access to change or add code to electronic equipment that is part of an electronic voting system has the ability to control the behavior of that equipment, such as the ability to cause the equipment to change, delete, or fabricate votes. *Id.* ¶ 34. A malicious program can be written to cause the device to perform tasks immediately, or at a conditional time in the future. *Id.* ¶ 22. A malicious program can modify other programs or data, delete other programs or data, or exfiltrate data on the device. *Id.* ¶ 23. Malicious programs can be configured to be extremely subtle, choosing not to alter all votes, or to only alter votes from specific precincts, on specific times or on specific days. *Id.* ¶ 36. They can even be configured to only be triggered after a certain type of ballot comes through, or a certain set of ballots in sequence. *Id.* A malicious program can even be written to delete *itself* after its instructions are completed. *Id.* ¶ 23.

Cybersecurity is the practice of ensuring the confidentiality, availability, and integrity of computerized devices and the data that resides on them. *Id.* ¶ 30. This includes preventing changes being made to the computer programs or data on a device by any person who is not authorized to made changes by the owner of the device, and detecting/remediating any unauthorized changes that are made. *Id.* Cybersecurity also requires establishing a "secure baseline" for the device, and maintaining adequate logs for the device, which record data about access to or changes made to it. *Id.* ¶¶ 25, 27. "Hacking" is the process by which the misconfiguration of a computerized device or erroneous code on the device is exploited to cause some adverse behavior that impacts the confidentiality, integrity or availability of the computerized device. *Id.* ¶ 32.

A malicious program can be written to delete traces that it ever ran, including deleting itself. Logan Decl. ¶ 23.

2. Electronic Devices in Voting Systems

In the context of Electronic Voting Systems, these principles have numerous implications. Any person who gains sufficient access to add or update a program on electronic equipment that is part of an Electronic Voting System has the ability to control the behavior of that equipment – such as the ability to cause the equipment to change, delete, or fabricate votes. Logan Decl. ¶ 34. Malicious actors who wish to control the outcome of an election without regard to the actual votes cast by voters can create, and save to the memory or storage of an electronic device, a malicious program that instructs the device to report that a particular candidate received a majority of the votes, or to report that votes cast for one candidate were instead votes cast for another candidate. *Id.* ¶ 35. To prevent electronic devices from manipulating votes, the devices must be absolutely secured against the introduction of any malicious programs. *Id.* ¶ 37. Programs must go through proper cybersecurity testing, and computerized devices must be configured to cybersecurity best practices so that access is controlled, systems are up-to-date with the latest patched versions of computer programs, and all actions on the system are properly logged so they can be validated. *Id.* ¶ 38.

Manufacturers of Electronic Voting Systems claim their products are secured against unauthorized access. However, at least one manufacturer, Dominion, has admitted that *any* computer can be hacked given enough time and access. Parker Decl. ¶ 7 & Ex. F at ¶ 13 (Declaration of Dr. Eric D. Coomer, then-Director of Product Strategy and Security for Dominion Voting Systems). A malicious program can be copied to Electronic Voting Systems through portable storage media, such as a USB device. Logan Decl.

¶¶ 24, 35. A malicious program can also be copied to an Electronic Voting System through a local network or through an internet connection. *Id.* ¶ 24. Malicious programs could even infiltrate an Electronic Voting System during the equipment manufacturing process, from data maliciously implanted on the physical components that constitute the equipment. Decl. of Shawn A. Smith ¶¶ 11-15 ("Smith Decl.").

3. General Vulnerability of Electronic Voting Systems

Electronic election equipment is notorious for continuing to be inadequately secure against intrusion even *after* federal government certification for use. In a 2021 article addressing the issue of errors and vulnerabilities in computer code, three professors of computer science cited voting machines as the "best-documented example" of "adversarial testing" finding "flaws in software that had been certified by outside parties." Steven M. Bellovin et al., *Seeking the Source: Criminal Defendants' Constitutional Right to Source Code*, 17 Ohio St. Tech. L. J. 1, 35 (Dec. 2020) (Parker Decl. ¶ 8 & Ex. G). "[O]utside auditors," they wrote, "have *always* found flaws" in voting machine software. *Id.* As a result, "There is broad consensus among elections experts that modern software systems are, by virtue of their design, too complex and unreliable to be relied upon for determining the outcomes of civil elections." *Id.* at 36-37.

A fourth professor of computer science testified in detail about these vulnerabilities before the Senate Select Committee on Intelligence in 2017. J. Alex Halderman, who had spent a decade studying electronic voting systems, testified that "our highly computerized election infrastructure is vulnerable to sabotage and even to cyber attacks that could change votes." He testified, "I know America's voting machines are vulnerable because my colleagues and I have hacked them repeatedly as part of a decade of research studying the technology that operates elections and learning how to make it stronger. We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies." *Russian Interference in the 2016 U.S. Elections* at 72, Hearing of S. Sel. Comm. on Intelligence, S.Hrg. 115-92 (June 21, 2017) (Parker Decl. ¶ 9 & Ex. H) ("Halderman Testimony"). Professor Halderman testified, "Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in *every single case*, they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes. That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk." *Id*. at 76 (emphasis in original).

On August 2, 2021, Professor Halderman signed a declaration for litigation concerning electronic voting systems used in Georgia. The declaration stated that Professor Halderman had spent twelve weeks performing intensive testing of Dominion voting equipment used in Fulton County, Georgia, and found "multiple severe security flaws," that attackers could exploit "to install malicious software, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems," and "such malware, once installed could alter voters' votes while subverting all the procedural protections practiced by the State." Decl. of J. Alex Halderman ¶ 4, *Curling v. Raffensperger*, no. 17-cv-2989-AT, ECF 1304-3 (N.D. Ga. Feb. 3, 2022) (Parker Decl. ¶ 10 & Ex. I).

After hearing Dr. Halderman's testimony and a large amount of other evidence, the federal court in the *Curling* litigation concluded, "Evidence presented in this case overall indicates the possibility generally of hacking or malware attacks occurring in voting systems and this particular system through a variety of routes - whether through physical access and use of a USB flash drive or another form of mini-computer, or connection with the internet. As discussed in the declarations and testimony of the proffered national cybersecurity experts in this case, a broad consensus now exists among the nation's cybersecurity experts recognizing the capacity for the unobserved injection of malware into computer systems to circumvent and access key codes and hash values to generate fraudulent codes and data. In these experts' views, these risk issues are in play in the operation of Dominion's Democracy Suite 5.5-A GA." *Curling v. Raffensperger*, 493 F. Supp. 3d 1264, 1280 (N.D. Ga. 2020).

Douglas Logan is an industry cybersecurity practitioner who has developed cybersecurity programs and led cybersecurity-related services for the federal government and Fortune 500 corporations, including malicious code detection, code review, threat modeling, and hacking vulnerability testing. Logan Decl. ¶¶ 3-5. He has also written training materials and taught classes on these topics. *Id.* ¶ 6. He has overseen or conducted application vulnerability assessments on over 2,000 software applications. *Id.* ¶ 8. Logan testifies:

- Commercially available voting machines from major vendors have for years been hacked by participants at an annual cybersecurity conference called DEFCON, including by participants with little prior knowledge and limited tools and resources. *Id.* ¶¶ 43-47. A variety of techniques have been demonstrated to allow an unauthorized person to change votes within the electronic election equipment, even new systems. *Id.* ¶ 47. The vulnerability to hacking includes equipment with a security vulnerability that was disclosed to the vendor a decade ago, yet never fixed by the manufacturer. *Id.* ¶ 45.
- Investigation of Dominion equipment used to administer the 2020 election in Antrim County, Michigan revealed that the election software could be easily

modified to attribute one candidate's votes to another candidate, the election software fell short of basic validation practices used even in commercial inventory control software, and the software could easily be intentionally modified to wrongly attribute votes to a favored candidate while outputting manipulated results on the poll tape, thereby leaving little indication that anything had been tampered with. *Id.* ¶¶ 48-54. After analyzing equipment used in Antrim County, post-election, Logan found the Dominion software exhibited a large number of failures in implementing secure coding practices, application security design principles, and cyber security best practices. *Id.* ¶ 57.

- Logan authored an evaluation, commissioned by the Arizona Senate, of the performance of Maricopa County, Arizona voting practices and equipment during the 2020 general election. *Id.* ¶¶ 10, 59. After reviewing the Dominion equipment and software used by Maricopa County, he concluded the software lacked necessary security measures; security logs that recorded access to the system had been lost and files deleted, often without any record of who performed these actions; and the system allowed multiple people to access it through shared accounts that did not change from year to year, thereby permitting changes to be made without any record of who made the changes. *Id.* ¶¶ 59-63 & Ex. E.
- "Air gap" cyber security practices are not sufficient to adequately protect election systems. *Id.* ¶¶ 81-84. First, there is substantial evidence that many election systems are not actually protected by air-gapping at all times. *Id.* ¶ 82. Second, even a properly air-gapped system can have malicious code copied to it through means other than a direct network connection, such as through a portable USB drive. *Id.* ¶¶ 83-84.

- After speaking with election workers across the country, Logan concluded that many election workers operating electronic equipment to administer elections have inadequate technical knowledge and rely fully on the equipment vendor or its subcontractors to perform the most basic tasks. *Id.* ¶¶ 12, 87-88.
- Considering the complexity of electronic election equipment and software, the general lack of cybersecurity sophistication of election workers, elected officials, and others, and the equipment's vulnerability to compromise, Logan has concluded that electronic voting systems cannot be properly secured by the 2022 elections and should not be used. *Id.* ¶¶ 85-91.

Col. (Ret.) John Mills served in senior positions in the Department of Defense, including Director of Cybersecurity Policy, Strategy, and International Affairs. Mills Decl. ¶¶ 2, 21. He has taught cybersecurity law and policy at the University of Maryland since 2013. *Id.* ¶ 2. He has also served as an election official at the county level. *Id.* ¶ 17, 22. Col. Mills testifies that "remote access operations" capability to access computer networks without detection have greatly expanded from the 1980s to the present. *Id.* ¶¶ 4-6, 27-45. The U.S. Government conducts remote access operations. *Id.* ¶ 7. Other countries, organizations, and individuals have capabilities to conduct remote access operations with varying degrees of sophistication, which have expanded at an accelerating rate over the last two decades. *Id.* ¶ 8. Electronic election infrastructure can be subjected to remote access operations that can change vote totals. *Id.* ¶¶ 9-10. Today, remote access operation capabilities have "escaped" from U.S. "classified environments" into "the wild," and other countries including China, Russia, Iran, North Korea, and Venezuela now use the same, similar, and improved methodologies. *Id.* ¶¶ 11, 15, 36. In view of successful cyberattacks now known to have succeeded against U.S. federal government targets and the state of the U.S. election process, Col. Mills concludes that federal government assertions about the 2020 election being "the most secure in American history" have "little, if any, basis in fact." *Id.* ¶¶ 18-19. American elections deviate substantively from the standards for free and fair elections, with respect to the operation of election machines and technology. *Id.* ¶¶ 46-48. After reviewing evidence concerning the election equipment used in Mesa County, Colorado for the 2020 election, Col. Mills finds the evidence "consistent with previous, publicly known, computer network intrusions, breaches, exfiltrations, and compromises of data integrity conducted via remote access operations by sophisticated actors, likely nation state level, with intimate, insider knowledge of the machines, networks, operating systems, and complete architecture of the information technology environment including off premise, 'cloud' based storage and processing." *Id.* ¶¶ 12-13, 20-21.

4. Supply Chain Vulnerability of Electronic Voting Systems

Yet another vulnerability in electronic election equipment is vulnerability to attack through the supply chain that produces the hardware and software used in the equipment. Shawn Smith is a retired U.S. military officer who served more than 25 years performing tasks related to the management of computer-based weapons systems, and who has served in his retirement as a consultant to the Department of Defense concerning cyber threat risks against U.S. governmental and non-governmental national security targets. Smith Decl. ¶¶ 2-6. Smith testifies that "U.S. elections are critically vulnerable to exploitation by foreign adversaries through supply chain compromise of our computerized election systems." *Id.* ¶ 8. A supply chain compromise is the deliberate introduction of flaws, covert access or functionality, malicious code, or other undesirable attributes into a product or service in the supply chain lifecycle of the product or service. *Id.* ¶ 12. A supply chain compromise may be intended to make a device accessible to unauthorized parties or to behave differently upon the occurrence of a command or specified conditions. *Id.* It can take place at any stage of the supply chain, going back to the design, integration, or manufacture of the product. *Id.* ¶¶ 13, 15. Supply chain attacks are now frequent occurrences in the global economy, and data indicate that in excess of 90% of companies surveyed have experienced a cybersecurity supply chain breach. *Id.* ¶ 14. "Supply chain attack is so pervasive that it must be assumed to threaten and affect all computers, computer components, hardware with embedded electronics, software, and firmware, to the extent that any aspect of them is accessible, at any time in their lifecycle from conception through end-of-life, to malicious or self-interested domestic or non-governmental actors but especially to foreign nation states and their agents." *Id.* U.S government entities and private sector organizations have publicized the increasing threat of supply chain attacks. *Id.* ¶¶ 15-18.

Supply chain attacks may take many different forms. *Id.* ¶ 23. CISA, the U.S. federal agency tasked with ensuring the cyber security of critical infrastructure in the United States, had *its own* computer networks compromised for at least ten months in 2020 by two separate supply chain attacks, and only learned of these attacks when notified of the threat by a private company. *Id.* ¶ 20. At least 120 sophisticated cyber threat groups, including arms of China's military, have been publicly identified. *Id.* ¶ 27. These groups enjoy the resources and support of foreign governments and have the capacity to pursue years- and decades- long campaigns to create and exploit supply chain vulnerabilities in targeted institutions and systems. *Id.* ¶¶ 28-37. U.S. government resources to defend electronic election systems against these cyber threats are sorely inadequate. *Id.* ¶¶ 40-63. None of the measures necessary to secure U.S. electronic voting systems against supply chain attacks have been in place. *Id.* ¶ 59. In view of the capacity of foreign cyber threat actors to accomplish supply chain attacks on U.S. election equipment systems, U.S. voting systems are not secure or securable. *Id.* ¶ 78. The electronic election equipment that Arizona intends to use in the 2022 Election uses components that may have been compromised by a supply chain attack, and such an attack, if it happened, may never be discovered. *Id.* ¶¶ 78-80 & Appendices.

5. Specific Examples of Vulnerable Electronic Voting Systems

Benjamin Cotton is a computer forensics professional with twenty-six years of experience performing computer forensics and digital systems analysis, including nearly two decades as an instructor of computer forensics and incident response. Decl. of Benjamin Cotton ¶¶ 4-5 ("Cotton Decl."). He has forensically examined Dominion Democracy Suite voting systems used in counties in four states, including Maricopa County, Arizona, and has reviewed the administrative manuals and documentation for the Dominion Democracy Suite software and hardware components. *Id.* ¶¶ 7, 9-10. He has also reviewed substantial other materials relating to EAC certification of election software and the performance of election software in the 2020 general election. *Id.* ¶¶ 11-15. In the course of these analyses, he found:

- The Democracy Suite systems in all four states had never received antivirus definition updates after the installation of the Democracy Suite software. *Id.* ¶ 18(a). Because an enormous amount of malicious code is continuously created and released, it is imperative to the security of any computing system that its antivirus definitions be updated as updates become available, typically on a weekly basis. *Id.* Because the Maricopa County antivirus definitions had not been updated, that system would not have prevented over 570,000,000 pieces of malicious code from compromising it.
- The Democracy Suite systems in all four states exhibited a consistent failure of the responsible authorities to implement operating system software patches at any time after the initial installation of the Democracy Suite software. The Democracy Suite

systems in all four states contained vulnerabilities that could be exploited to gain unauthorized access to the systems. *Id.* ¶ 18(b). There was no evidence on the systems of a procedure to patch or fix operating system vulnerabilities. *Id.* The Maricopa County systems had not been patched for 19 months, a period during which 3,512 Windows vulnerabilities were identified. *Id.* & Cotton Decl. Ex. J.

- Each Democracy Suite system used identical passwords for all user accounts on that particular system, and the passwords were never changed after initial installation of the software. *Id.* ¶ 18(c). Further, the user accounts did not appear to be assigned to specific individual people. *Id.* CISA and industry best practices recommend all username and password combinations be unique and assigned to one individual, with access disabled for users who no longer require access and with passwords changed every ninety days. *Id.* This means there was "long-term shared password exposure for multiple elections," and "individual accountability for actions performed by the account during an election" was "impossible." *Id.*
- None of the systems in the four states had the capability to actively monitor the programs that were running on the computers or monitor network activity. *Id.* ¶ 18(d). Nor did they have a process to alert election officials if activity deviating from an approved, expected baseline occurred. *Id.* Accordingly, system administrators would not know if an unauthorized person gained access to the voting systems and either caused them to carry out improper functions or concealed code within them to cause them to carry out improper functions in the future.
- All four systems lacked adequate log management practices. *Id.* ¶ 18(e). Software logs create a record of instances in which a person gained access to the system and the activities performed within the system. Logan Decl. ¶ 27. "[A] robust log

management program support[s] the detection and monitoring of real-time security postures," and "in the event of an audit or a cyber security event," the logs "support triage and remediation of the historical cybersecurity events." Cotton Decl. ¶ 18(e). Secure logs are a critical cybersecurity function. *Id*. Failing to ensure adequate log management can result in a situation where the data needed to determine if a breach occurred does not exist. Logan Decl. ¶ 27. The logs in the voting systems in all four states were exposed to modification by users, meaning that an unauthorized user could make changes to the system and then delete the log entries that recorded the unauthorized access. *See* Cotton Decl. ¶ 18(e)(ii). "It is common for threat actors to delete, modify and/or otherwise manipulate logs and other artifacts as an integrated elements of an unauthorized attack," and therefore "[a]n effective log management program would establish a centralized log repository that is not located on the device that generates the logged event." *Id.* ¶ 18(e)(i). Further, the logs were configured so that their entries would be automatically overwritten after a certain number of events were recorded. *Id*. ¶ 18(e)(iv). As a result, the mere passage of time and operation of the system would result in the loss of important log data. In Maricopa County, the critical Windows security.evtx log file had so many entries overwritten that by the time Cotton examined it, the log only recorded events occurring on February 5, 2021 and later – meaning the log entries from the 2020 election had been destroyed. *Id.*

- The Democracy Suite voting systems in all four states attempted to segment the equipment that recorded votes from other administrative support equipment. *Id*. ¶ 18(f). However, the form of segmentation was an "air gap" configuration. *Id*. Air gapping can be easily bypassed by connecting any one of a number of devices (including a cell phone) to the air gapped system. *Id*. Further, the computers in the

Democracy Suite system are commercial off-the-shelf equipment that contain wireless 802.11 modems that can connect the computers to an unauthorized network, and the systems did not have any mechanism to detect or prevent such a security violation from occurring. *Id.*

- The Democracy Suite voting systems lacked any mechanism for blocking malicious activity or programs, aside from the outdated antivirus program. *Id.* ¶ 18(g). The systems do not have the ability to detect or block suspicious activity. *Id.*
- "Administrative access" to a computer or computer system means a person knows the necessary passwords to access critical functions of the software and make authorized changes to the software. Logan Decl. ¶ 33. "Administrative access" gives a person control over the computer or system without needing to hack it. *Id.* The county officials with responsibility to administer the voting systems typically lacked administrative access to their own equipment, instead leaving administrative access solely within the control of employees of the vendor who supplied the equipment, such as Dominion. Cotton Decl. ¶ 19. Maricopa County officials lacked administrative access to Maricopa County's equipment. *Id.* The county officials had no way to independently verify that these contracted employees were properly performing their tasks, were not exposing the systems to unauthorized access, or had properly configured the system. *Id.*
- The voting systems in the four states would not have been certifiable under PCI or HIPAA industry standards. *Id.* ¶ 20.

6. Historical Breaches of Election-Related and Government Cyber Security

Multiple past instances of election-related and government computers being hacked have been discovered.

In 2020, CISA, the U.S. federal agency responsible for the cybersecurity of critical infrastructure including electronic election equipment, was *itself* victimized for over ten months by two hacks of its own computer networks that it did not discover until it was informed of them by a private company. Smith Decl. ¶ 20.

Georgia's state election server was breached, exposing voter data, software passwords, and software applications to the public. *Curling*, 493 F. Supp. 3d at 1273-74.

The U.S. Senate Select Committee on Intelligence issued a report titled *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views* (Parker Decl. ¶ 11 & Ex. J). While the publicly available version of the report is heavily redacted, it reveals the following: "The Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure at the state and local level." *Id*. at 3. The report used the term "election infrastructure" to refer to "the equipment, processes, and systems related to voting, tabulating, reporting, and registration." *Id*. At least 21 states were targeted. *Id*. at 15-20. Russian cyber actors successfully penetrated Illinois's voter registration database and accessed up to 200,000 records, obtaining an unknown quantity of voter registration data. *Id*. at 22. The Russian actors could have deleted or changed voter data, but it does not appear they did so. *Id*. "Election infrastructure" in another state was also breached by Russian cyber actors, but details regarding this incident were redacted. *Id*. at 24. Russian cyber activity was also directed at "Voting Machine Companies," but details regarding this activity were redacted. *Id*. at 29-30.

Dr. Walter Daugherity taught in the Department of Computer Science and Engineering at Texas A&M University for over thirty years. Decl. of Walter C.

Daugherity ¶¶ 1-2 ("Daugherity Decl."). Dr. Daugherity examined the Cast Votes Records from Pima County, Arizona and Maricopa County, Arizona for the 2020 election. *Id*. ¶¶ 6-7. Focusing on the early mail-in and in-person votes, he found that the ratios of votes for one candidate to another exhibited a systematic decline over time, as each batch successively closer to election day showed a lower ratio. *Id*. ¶¶ 9-35. He concluded, "Such predictability and dependence would not occur without artificial manipulation. Achieving such predictability requires what should be independent votes to be artificially manipulated to form the downward sloping line for the cumulative vote ratio. In my expert opinion such predictability is so statistically improbable as to be impossible and thus demonstrates to a reasonable degree of scientific and mathematical certainty that the tabulation of these ballots was artificially controlled." *Id*. ¶ 31. Rather, "[t]he standard method of producing such control . . . is to use a Proportional-Integral-Derivative (PID) controller in a closed-loop feedback system," a technique broadly used in other contexts including cruise controls in automobiles and industrial automation of all kinds. *Id*. ¶¶ 34-35, 7-8. Dr. Daugherity was able to program a PID controller "to produce the observed cumulative ratio" with "good convergence." *Id*. ¶ 36.

C. <u>Administrative Cybersecurity Risks.</u>

Even in a well-designed computer system the factor of human error can lead to cybersecurity breaches. Logan Decl. ¶ 40. Ultimately it is individual employees or officials who must choose secure passwords, keep their passwords secret, refrain from activating malware by opening email attachments or clicking on unsafe internet links, refrain from connecting computer hardware to portable computer memory media or computer networks, maintain software up-to-date, and a host of other mundane cybersecurity practices – including remembering what cybersecurity practices must be observed. *Id*. ¶ 41. Experience has shown that humans err on these practices, through ignorance, forgetfulness, neglect, and even intention, simply because it is less demanding to ignore the proper procedure. *Id.* ¶ 42. County election officials who use election equipment only a handful times in each two-year election cycle, together with volunteer election workers who may not have much cybersecurity training, present prime candidates for cybersecurity breach as a result of human factors. "I have never come across a county where the sworn election officials know how to access or see network activity beyond the operator level of any election machine or related information technology component." Mills Decl. ¶ 47. On balance, Col. Mills believes based on his experience that "the U.S. Government does not have the people, programs, or resources to have a comment on the true resilience and security of the election critical infrastructure." *Id.* ¶ 50.

D. <u>Electronic Voting System Manufacturers Not Reliable.</u>

The manufacturers of electronic voting systems cannot be relied upon to provide quality equipment reasonably secure against unauthorized intrusion and manipulation.

The U.S. Election Assistance Commission (EAC) was created by Congress in 2002 to test and certify voting systems. 52 U.S.C. §§ 20921-20922. On March 20, 2020, EAC issued a letter to ES&S stating that ES&S had misrepresented the certification of its voting systems by the EAC.[3] The misrepresentation related to the inclusion of optional modems in some election equipment manufactured by ES&S, but referring in marketing materials to the equipment with optional modems as "fully certified and compliant with EAC guidelines." *Id.*

On November 3, 2021, the EAC received a report from the Tennessee Secretary

[3] Kim Zetter, POLITICO, Aug. 13, 2020, *Election commission orders top voting machine vendor to correct misleading claims*, *available at* https://www.politico.com/news/2020/08/13/election-voting-machine-misleading-claims-394891; https://www.politico.com/f/?id=00000173-e9b5-d0bf-a17b-fdbfc0290000.

of State related to an anomaly from the October 26, 2021, municipal elections in Williamson County, Tennessee. Logan Decl. ¶ 65. Votes counted by 7 of the 18 ballot scanners did not match the number of ballots scanned. *Id.* During a subsequent investigation, the anomaly was reproduced and connected to error codes in the equipment logs, but the cause of the erroneous behavior could not be determined by the investigation team that included two EAC accredited vendors and representatives from Dominion, the EAC, the Tennessee Secretary of State, and Williamson County. *Id.* ¶¶ 66-69. Later, Dominion submitted an analysis to the EAC stating "erroneous code is present in the EAC certified D-Suite 5.5-B and D-Suite 5.5-C systems." *Id.* ¶ 70. Dominion stated that when a certain part of a QR code was misread, the ICP interpreted the ballot as provisional and thereafter marked all ballots subsequently scanned as provisional, leaving these ballots out of the close poll report totals. *Id.* Dominion's solution was to submit revised code that would reset the provisional flag within the tabulator after a ballot was scanned as provisional, so that subsequent ballots would not automatically be flagged as provisional. *Id.* Because of the features and characteristics of QR codes, Dominion's explanation is insufficient to adequately explain what occurred. *Id.* ¶¶ 70-74. Moreover, Dominion's code change did not fix the cause of the ballot misreads – it simply reset the provisional flag so the error code would not impact subsequently scanned ballots. *Id.* ¶ 75. Overall, the EAC report concerning Dominion election equipment in Williamson County, Tennessee shows that "erroneous code" was included in the Dominion system actually used in the election, the same code has been used in elections across the country for some time, with unknown impact on elections in other locations, the EAC accepted an explanation from Dominion that does not make technical sense, and the EAC deferred to the vendor to define the root cause and create code to fix the issue. *Id.* ¶ 80.

The system used in Williamson County, Tennessee was the Dominion D-Suite 5.5-

B system. *Id.* ¶ 66. Maricopa County intends to use a Dominion D-Suite 5.5-B system for the 2022 Election. Parker Decl. ¶ 2 & Ex. A.

CISA issued a public statement concerning a Dominion voting system used in sixteen states, including Arizona. The statement detailed a number of critical vulnerabilities discovered by a computer scientist in connection with litigation to prohibit the use of the electronic voting machines used in Georgia.[4]

E. <u>Hand Voting and Counting With Paper Ballots Is Practical.</u>

Returning to voting by auditable paper ballots counted by hand is safe, secure, and reasonable. It is the method used in past U.S. elections. It is a method approved for use by Arizona statute. "If for any reason it becomes impracticable to count all or a part of the ballots with tabulating equipment, the officer in charge of elections may direct that they be counted manually." A.R.S. § 16-621(C). It is the method successfully used today by voters in other countries. Taiwan, under constant geopolitical pressure from China, for its 2020 election used manual counting to the greatest degree possible, the simplest of election machines and technology, and counting in full view on Jumbo-Tron screens so observers could see the ballot and how the count changed with each ballot. Mills Decl. ¶¶ 23-26.

For many years, prior to the invention of mechanical or computerized election equipment, American voters cast hand-marked paper ballots and counted the vote totals by hand. Today's citizens are just as capable of that process as their forebears. Counting

[4] *Curling et al. v. Raffensperger et al.*, No. 1:17-CV-2989-AT, ECF 1391 (N.D. Ga. June 4, 2022). CISA's statement is available at https://www.cisa.gov/uscert/ics/advisories/icsa-22-154-01.

votes by hand, in individual precincts, is neither unrealistic nor unprecedented.

II.
PRELIMINARY RELIEF IS NECESSARY

The Constitution requires that elections be free, fair, and accurately counted. Changing reported votes or vote totals in a public election violates Plaintiffs' fundamental right to vote and Plaintiffs' rights under the Due Process clause and the Equal Protection clause. The only way to prevent these violations is to refrain from using vulnerable Electronic Voting Systems to administer future elections, including the 2022 Election. The relief requested by Plaintiffs is the only way to eliminate the likelihood that Arizona's election results from will be secretly changed by malicious programs hidden in Electronic Voting Systems. Accordingly, a preliminary injunction is appropriate and necessary to remedy the impending violations of Plaintiffs' constitutional rights.

"In order to obtain a preliminary injunction a plaintiff must establish (1) 'that he is likely to succeed on the merits,' (2) 'that he is likely to suffer irreparable harm in the absence of preliminary relief,' (3) 'that the balance of equities tips in his favor,' and (4) 'that an injunction is in the public interest.'" *Hernandez v. Sessions*, 872 F.3d 976, 989-90 (9th Cir. 2017) (quoting *Winter v. NRDC, Inc.*, 555 U.S. 7, 20 (2008)). "Under our 'sliding scale' approach, 'the elements of the preliminary injunction test are balanced, so that a stronger showing of one element may offset a weaker showing of another.'" *Hernandez*, 872 F.3d at 990 (quotations omitted). Plaintiffs meet each of the four elements here.

A. <u>Plaintiffs Are Likely to Succeed on the Merits.</u>

Plaintiffs will prevail on the merits of their claims because the right to vote and have one's vote counted correctly together with all other votes is a basic right guaranteed by multiple constitutional provisions, and the use of Electronic Voting Systems as Arizona intends grossly infringes that right.

1. Plaintiffs Have a Constitutional Right to Have Their Votes Cast and Counted Through an Election System Not Subject to Vote Manipulation.

Voting is, indisputably, a right "of the most fundamental significance under our constitutional structure." *Burdick v. Takushi*, 504 U.S. 428, 433 (1992) (internal quotation marks and citation omitted). "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *Wesberry v. Sanders*, 376 U.S. 1, 17 (1964). Therefore, states may not, by arbitrary action or other unreasonable impairment, burden a citizen's right to vote. *Baker v. Carr*, 369 U.S. 186, 208 (1962) ("citizen's right to a vote free of arbitrary impairment by state action has been judicially recognized as a right secured by the Constitution"). "A law that severely burdens the right to vote must be narrowly drawn to serve a compelling state interest." *Curling*, 493 F. Supp. 3d at 1280 (citing *Burdick*, 504 U.S. at 434). "Since the right to exercise the franchise in a free and unimpaired manner is preservative of other basic civil and political rights, any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized." *Reynolds v. Sims*, 377 U.S. 533, 562 (1964).

The scope of the right to vote requires states to adopt methods of voting, vote collection, vote counting, and vote tallying that ensure fair, accurate, and secure counting of all legal ballots and exclude any attempt to change the total results reported to differ from the true sum of the votes legally cast. The fundamental right to vote is "the right of qualified voters within a state to cast their ballots and have them counted." *United States v. Classic*, 313 U.S. 299, 315 (1941). It necessarily encompasses the right to have **all** votes counted accurately. "Every voter's vote is entitled to be counted once. It must be correctly counted and reported." *Gray v. Sanders*, 372 U.S. 368, 380 (1963). Because the significance of a vote is inherently comparative – the meaning of a vote is destroyed by improper inflation of opposing vote totals, just as much as if the vote itself was wrongfully prevented – a state's entire system of collecting, counting, and tallying votes must prevent any manipulation of the reported totals. "[T]he right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise." *Reynolds*, 377 U.S. at 555. *See also United States v. Saylor*, 322 U.S. 385, 386 (1944) ("'[T]he free exercise and enjoyment of the rights and privileges guaranteed to the citizens by the Constitution and laws of the United States'" entails "the right and privilege . . . to have their expressions of choice given full value and effect by not having their votes impaired, lessened, diminished, diluted and destroyed by fictitious ballots fraudulently cast and counted, recorded, returned, and certified.").

The framework articulated by the Supreme Court in *Anderson v. Celebrezze*, 460 U.S. 780 (1983) and *Burdick*, 504 U.S. 428 is used to resolve the "competing constitutional commands" of the right to vote and "the practical realities of voting laws." *Ariz. Democratic Party v. Hobbs*, 18 F.4th 1179, 1186 (U.S. 9th Cir. 2021). *Anderson/Burdick* applies a "flexible standard" that weighs the character and magnitude of the asserted injury against the interests put forward by the state to justify the burdens imposed by its law. *Id*. Here, the injury is maximum; Defendants' use of Electronic Voting Machines in practical effect completely denies voters their right to vote, by allowing the outcome of elections to be solely determined by a cyber intruder who manipulates the electronic election equipment. Under Defendants' system, it does not matter how Plaintiffs or anyone who shares their interests votes, because the "winner" of the election may not be determined by votes at all, but rather solely by the manipulation of a cyber intruder. There is no interest the State could advance to justify blanket nullification of the right to vote in this manner. The outcome of an *Anderson/Burdick* analysis clearly supports the relief Plaintiffs seek.

A voting system that counts ballots cast by some voters using different standards from ballots cast by other voters also violates the Equal Protection rights of the voters. “Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person’s vote over that of another.” *Bush v. Gore*, 531 U.S. 98, 104-05 (2000); *Dunn v. Blumstein*, 405 U.S. 330, 336 (1972) (“[A] citizen has a constitutionally protected right to participate in elections on an equal basis with other citizens in the jurisdiction.”).

Federal courts are obligated to intervene to correct state voting practices found to infringe the right to vote, and to prevent future elections from using such practices. “Once a State’s [election-related] scheme has been found to be unconstitutional, it would be the unusual case in which a court would be justified in not taking appropriate action to insure that no further elections are conducted under the invalid plan.” *Reynolds*, 377 U.S. at 585. If Arizona’s voting system permits a person – any person – to surreptitiously change, inflate, or diminish vote totals so that they differ from the true totals of the legal votes cast, then Arizona’s voting system infringes the constitutional rights of Plaintiffs to vote. If Arizona’s system counts ballots cast by absentee voters securely, but counts ballots cast at polls insecurely (or *vice versa*), the system infringes the Equal Protection rights of the Plaintiffs. Indeed, if Arizona counts ballots cast by absentee voters differently than it counts ballots cast at polls, the system infringes those same Equal Protection rights.

2. Arizona’s Use of Electronic Voting Systems Permits Vote Manipulation.

Electronic Voting Systems are inherently vulnerable to improper manipulation of votes and vote totals. They cannot be effectively secured against improper manipulation. Therefore, they cannot be constitutionally used to administer Arizona's elections.

i. Electronic Voting Systems Can Be Controlled by Unauthorized Persons Through the Introduction of Malicious Computer Programs.

A person who gains sufficient access to electronic equipment that is part of an electronic voting system to add or update a program on it thereby gains the ability to control the behavior of that equipment. Logan Decl. ¶ 34. Programs can be written to cause an Electronic Voting System to change the votes cast by a voter, or to report vote totals different from the votes actually cast by voters. *Id*. ¶¶ 35-36. Such a program can be configured to only trigger upon subtle circumstances, making it impossible to detect in a Logic and Accuracy test. *Id*. The *only* way to ensure an Electronic Voting System reports correct votes and vote totals is to absolutely secure the system against the introduction of any malicious programs. *Id*. ¶ 37. A malicious program can be introduced onto a computerized device in numerous ways, including through a computer network or through portable storage media such as a USB device. *Id*. ¶ 24. It could also be hidden in the hardware or software components of the system at the time those components were manufactured. Smith Decl. ¶¶ 11-15.

ii. The Electronic Voting Systems That Arizona Intends to Use in the 2022 Election Are Inherently Vulnerable to the Introduction of Malicious Computer Programs.

The computer components of the Electronic Voting Systems that Arizona intends to use in the 2022 Election are not absolutely secured against the introduction of malicious programs, nor can they realistically be made secure. Logan Decl. ¶¶ 36, 39-42, 82-84, 90-91; Smith Decl. ¶¶ 39-40, 59, 80-81. Malicious programs could be introduced to them in multiple ways, including through an internet connection, over a wireless network, or through portable storage media. Logan Decl. ¶¶ 82-84, Cotton Decl. ¶ 18(f). The possibility of malicious code on portable storage media means that even "air-gapping" computerized equipment (attempting to prevent it from any connection to an external computer network) does not provide an adequate defense against the introduction of malicious programs. Logan Decl. ¶¶ 81-84. In fact, individual hardware components of a computer can be manufactured with malicious computer code written into them before the components are even installed into the computer during the manufacturing process, and then this code may instruct the computer to open itself up to access by an outsider in the future, permitting the introduction of additional malicious code. Smith Decl. ¶¶ 11-15, 39, 43. The use of this technique to compromise during the manufacturing process a computer's defenses against outside manipulation has become endemic in recent years, with over 90% of companies surveyed reporting a negative impact from such attacks. *Id.* ¶ 14. In 2020, the U.S. federal agency responsible for the cybersecurity of critical infrastructure, CISA, was itself victimized for over ten months by two supply chain attacks that it did not discover until it was informed of them by a private company. *Id.* ¶ 20.

iii. Malicious Computer Programs Can Change the Reported Results of an Election Without Leaving Any Evidence of the Change.

Strategically constructed malicious programs can cause a computer to erase the traces of them, and the malicious programs themselves, after they complete their work. Logan Decl. ¶ 23. This means that a person who sought to change election results could transmit a program to an Electronic Voting System that caused the computers to change or inflate vote totals so that a specific candidate was reported to receive the most votes, and then *delete the malicious program*, leaving no evidence that the election results were changed. If this happened, there would be no way to discover, from examination of the affected computer, that anything improper had occurred. Cotton's inspection of Dominion systems showed that these systems lacked any mechanism to detect or prevent a violation of system security by any user who knew the shared password for the system in a "matter of seconds," or to detect or block suspicious activity at all. Cotton Decl. ¶ 18(f), (g). In Maricopa County, the electronic election equipment had election data purged and files deleted after the 2020 election, without any ability to attribute that activity to a specific individual. Logan Decl. ¶¶ 61(c), 63. This equipment was vulnerable to malicious programs because of multiple failures to implement cybersecurity practices. Cotton Decl. ¶ 18. The Maricopa network would not have been certifiable under PCI or HIPAA industry standards. *Id.* ¶ 20.

iv. Measures Intended to Secure Electronic Voting Systems Against Manipulation by Unauthorized Persons Are Not Effective.

As described above, Electronic Voting Systems are inherently vulnerable to unauthorized access and manipulation. Professor Halderman further explains, "Some say the fact that voting machines aren't directly connected to the Internet makes them secure, but unfortunately, this is not true. Voting machines are not as distant from the Internet as they may seem. Before every election, they need to be programmed with races and candidates. That programming is created on a desktop computer, then transferred to voting machines. If Russia infiltrated these election management computers, it could have spread a vote stealing attack to vast numbers of machines." Halderman Testimony at 72. Both in theory and in practice, the Electronic Voting Systems that Arizona seeks to use are not reliable or secure. Halderman, addressing Dominion Ballot Marking Device

(BMD) electronic election equipment used in Georgia, testified, "[T]he scientific evidence about voter verification shows that attackers who compromise the BMDs could likely change individual votes and even the winner of a close race without detection. Georgia can eliminate or greatly mitigate these risks by adopting the same approach to voting that is practiced in most of the country: using hand-marked paper ballots and reserving BMDs for voters who need or request them. Absent security improvements such as this, it is my opinion that Georgia's voting system does not satisfy accepted security standards." Halderman Decl. ¶ 33, ECF #1304-3, *Curling v. Raffensperger*, no. 1:17-CV-2989-AT (N.D. Ga. Feb. 3, 2022).

3. Arizona's Current System Does Not Protect Against Vote Fraud Through Hacking of Electronic Election Equipment.

Under Arizona law, "An electronic voting system consisting of a voting or marking device in combination with vote tabulating equipment shall provide facilities for voting for candidates at both primary and general elections." A.R.S. § 16-446(A). The electronic voting system must "Provide a durable paper document that visually indicates the voter's selections, that the voter may use to verify the voter's choices," and this "paper document shall be used in manual audits and recounts." *Id.* § 16-446(B)(7). The board of supervisors is required to "prepare and provide ballots" for the election, at county expense, except for local elections. *Id.* § 16-503. The counting of the ballots at the counting center is "under the direction of the board of supervisors or other officer in charge of elections." *Id.* § 16-621(A). If counting is performed using automatic tabulating equipment, only two percent of precincts are required to be counted by hand. *Id.* § 16-602(B)(1). But such a limited post-election hand count is not an effective means of detecting fraud, because the number of ballots counted is too small and because the method Arizona mandates for conducting the hand count, the "Sort-and-Stack" method, is known to be error-prone. Smith Decl. ¶¶

75-77.

For example, if one or even a few locations in an Arizona county had their electronic voting systems hacked to change votes, there is little chance that the fraud would be discovered by a hand count of the paper ballots at only two percent of precincts. This system does not reasonably ensure that Plaintiffs' constitutional right to vote is secure. On the contrary, it provides a great likelihood the violation of the Plaintiffs' constitutional rights would pass undetected.

B. Plaintiffs Will Suffer Irreparable Harm Absent Preliminary Relief.

"It is well established that the deprivation of constitutional rights 'unquestionably constitutes irreparable injury.'" *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012) (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976)); *Hernandez*, 872 F.3d at 994-95. Because Arizona's intended use of Electronic Voting Systems in the future elections, including the 2022 Election, will deprive Plaintiffs of their constitutional rights, they will suffer irreparable harm absent the grant of preliminary relief.

C. The Balance of Equities Favors an Injunction.

The balance of equities favors entering the injunction sought by Plaintiffs. It will cause little, if any, harm to the Defendants, because the system currently intended to be used already requires the creation of paper ballots for each voter, and the counting of the paper ballots by hand at 2% of precincts. *See* A.R.S. § 16-602(B). By Arizona law, the Defendants are already able to carry out the relief sought by Plaintiffs. The requested injunction would merely require the use of hand counting for all voters and all contests.

In contrast, failing to enter the injunction and permitting use of the currently intended system would inflict immeasurable harm. In addition to the deprivation of Plaintiffs' constitutional rights, the true election results would never be known with certainty, casting a pall of illegitimacy over the subsequent official acts of the winning candidates. If the defining feature of self-government is the selection of governing officials by majority vote, then conducting an "election" process in which it is not and *cannot* be confidently known which candidate actually received the majority vote means intentionally casting aside self-government. That enormous harm would be felt by all persons, whether citizen, voter, or neither, because it would bring into dispute the governance of the public authorities. The resulting loss of legitimacy and increase in political strife would be felt by all.

D. <u>The Requested Injunction Is in the Public Interest.</u>

The public interest requires free, fair, and accurately counted elections, in which the votes of all legal voters are counted equally and are not diluted by altered votes or phantom votes. This is also the constitutional right of Plaintiffs and all Arizona voters. "Generally, public interest concerns are implicated when a constitutional right has been violated, because all citizens have a stake in upholding the Constitution." *Hernandez*, 872 F.3d at 996 (quoting *Preminger v. Principi*, 422 F.3d 815, 826 (9th Cir. 2005)). Further, eliminating even the *appearance* of unsecure elections serves the public interest. "[P]ublic confidence in the integrity of the electoral process has independent significance, because it encourages citizen participation in the democratic process." *Crawford v. Marion Cnty. Election Bd.*, 553 U.S. 181, 197 (2008).

The use of Electronic Voting Equipment creates large, invisible risks of vote dilution and/or alteration. Therefore, the injunction against the use of this equipment sought by Plaintiffs strongly serves the public interest.

The principle that a federal court should not cause confusion among voters by enjoining state election laws immediately before an election, *Purcell v. Gonzalez*, 549 U.S. 1 (2006), does not apply in these circumstances. First, the 2022 Election is more than four months away, not bare weeks, as in *Ariz. Democratic Party v. Hobbs*, 976 F.3d 1081, 1086-87 (9th Cir. 2020) and the cases cited therein. "When an election is 'imminen[t]' and when there is 'inadequate time to resolve . . . factual disputes,'" *Purcell* will "often" (though "not always") prompt courts to "decline to grant an injunction to alter a State's established practice." *Ohio Republican Party v. Brunner*, 544 F.3d 711, 718 (6th Cir. 2008). The 2022 Election is upcoming, but not so imminent that inadequate time remains to allow for the relief sought by Plaintiffs.

Second, the "concerns that troubled the Supreme Court in *Purcell* are not present in this instance," where voters "will be entirely unaffected by an order enjoining" the disputed practice because it "applies only after a ballot is submitted." *Self Advocacy Sol. N.D. v. Jaeger*, 464 F. Supp. 3d 1039, 1055 (D.N.D. 2020). The relief sought by Plaintiffs here only affects the counting of the cast ballots – it does not affect the location of polling places, voter identity requirements, or any other matter that might prevent a voter from voting. All voters will be able to cast their ballots by appearing at the same poll locations just as they would in the absence of an injunction, so *Purcell*'s policy of preventing voter confusion is not applicable here. *See also Common Cause Ind. v. Lawson*, No. 1:20-cv-01825-RLY-TAB, 2020 U.S. Dist. LEXIS 247756, at *13 (S.D. Ind. Oct. 9, 2020) ("But the concerns animating *Purcell* and its progeny are not present in this case. This court's decision to preliminarily enjoin the Challenged Amendments poses little risk of disrupting Indiana's election process or confusing voters. The laws only pertain to Election Day activities, so they have no effect on any aspect of the election process up until then; any ongoing early voting activity is unaffected by the injunction."). Here, as in "many election-related disputes" that may occur even as late as "*on* election day" or "*during* election week," it is "unclear" why *Purcell* would apply – and so the court need not refrain from granting injunctive relief. *Ohio Republican Party v. Brunner*, 544 F.3d at 718. On the contrary, in light of the clear risk that illegal manipulation of vote totals may occur through unauthorized access to electronic election equipment, another policy affirmed by *Purcell* weighs in favor of *granting* injunctive relief:

> Confidence in the integrity of our electoral processes is essential to the functioning of our participatory democracy. Voter fraud drives honest citizens out of the democratic process and breeds distrust of our government. Voters who fear their legitimate votes will be outweighed by fraudulent ones will feel disenfranchised. "[T]he right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise." *Reynolds* v. *Sims*, 377 U.S. 533, 555 (1964).

Purcell, 549 U.S. at 4.

III.
CONCLUSION

For the foregoing reasons, Plaintiffs are entitled to a preliminary injunction prohibiting the use of Electronic Voting Systems to count the ballots or otherwise administer future Arizona elections.

DATED: June 8, 2022.

PARKER DANIELS KIBORT LLC

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

OLSEN LAW, P.C.

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

By */s/ Alan M. Dershowitz*
Alan M. Dershowitz (MA Bar No. 121200)#
1575 Massachusetts Avenue
Cambridge, MA 02138
To be admitted *Pro Hac Vice*

Counsel for Plaintiffs Kari Lake
and Mark Finchem

CERTIFICATE OF SERVICE

I hereby certify that on June 8, 2022, I electronically transmitted the foregoing document to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the CM/ECF registrants on record.

/s/ Andrew D. Parker

Query Reports Utilities Help Log Out

STD

U.S. District Court
DISTRICT OF ARIZONA (Phoenix Division)
CIVIL DOCKET FOR CASE #: 2:22-cv-00677-JJT

Lake et al v. Hobbs et al
Assigned to: Judge John J Tuchi
Cause: 42:1983 Civil Rights Act

Date Filed: 04/22/2022
Jury Demand: Plaintiff
Nature of Suit: 441 Civil Rights: Voting
Jurisdiction: Federal Question

Plaintiff

Kari Lake represented by

Andrew D Parker
Parker Daniels Kibort LLC - Minneapolis, MN
123 N 3rd St., Ste. 888
Minneapolis, MN 55401
612-355-4100
Fax: 612-355-4101
Email: parker@parkerdk.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kurt B Olsen
Olsen Law PC
1250 Connecticut Ave. NW, Ste. 200
Washington, DC 20036
202-408-7025
Email: ko@olsenlawpc.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alan M Dershowitz
Harvard Law School
1575 Massachusetts Ave.
Cambridge, MA 02138
617-496-2187
Email: dersh@law.harvard.edu
TERMINATED: 05/18/2022

Plaintiff

Mark Finchem represented by

Andrew D Parker
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kurt B Olsen
(See above for address)

LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alan M Dershowitz
(See above for address)
TERMINATED: 05/18/2022

V.

Defendant

Katie Hobbs
named as Kathleen Hobbs, as Arizona Secretary of State

represented by

Christine Bass
States United Democracy Center - Oakland, CA
5917 Contra Costa Rd.
Oakland, CA 94618
309-242-8511
Email: christinebass@statesuniteddemocracy.org
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Andrew Gaona
Coppersmith Brockelman PLC
2800 N Central Ave., Ste. 1900
Phoenix, AZ 85004
602-381-5481
Email: Agaona@cblawyers.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristen Michelle Yost
Coppersmith Brockelman PLC
2800 N Central Ave., Ste. 1900
Phoenix, AZ 85004
602-381-5478
Fax: 602-224-6020
Email: kyost@cblawyers.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Roopali H Desai
Coppersmith Brockelman PLC
2800 N Central Ave., Ste. 1900
Phoenix, AZ 85004
602-381-5478
Fax: 602-224-6020
Email: rdesai@cblawyers.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Sambo Dul

States United Democracy Center - Tempe, AZ
8205 South Priest Dr., Ste. #10312
Tempe, AZ 85284
480-253-9651
Email: bo@statesuniteddemocracy.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Bill Gates
as a member of the Maricopa County Board of Supervisors

represented by

Emily Mae Craiger
Burgess Law Group
3131 E Camelback Rd., Ste. 224
Phoenix, AZ 85016
602-806-2104
Email: emily@theburgesslawgroup.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph James Branco
Maricopa County Attorney Civil Services Division
225 W Madison St.
Phoenix, AZ 85003
602-506-8541
Fax: 602-506-8567
Email: brancoj@mcao.maricopa.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Eugene LaRue
Maricopa County Attorneys Office - Madison St.
225 W Madison St.
Phoenix, AZ 85003
602-506-8541
Fax: 602-506-8567
Email: ca-civilmailbox@mcao.maricopa.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Karen J Hartman-Tellez
Maricopa County Attorney Civil Services Division
225 W Madison St.
Phoenix, AZ 85003
602-526-6806
Email: hartmank@mcao.maricopa.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Thomas P Liddy
Maricopa County Attorneys Office - Civil

Services Division
222 N Central Ave., Ste. 1100
Phoenix, AZ 85004
602-506-8541
Fax: 602-506-8567
Email: liddyt@mcao.maricopa.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Clint Hickman
as a member of the Maricopa County Board of Supervisors

represented by **Emily Mae Craiger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph James Branco
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Eugene LaRue
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Karen J Hartman-Tellez
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Thomas P Liddy
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Jack Sellers
as a member of the Maricopa County Board of Supervisors

represented by **Emily Mae Craiger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph James Branco
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Eugene LaRue
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Karen J Hartman-Tellez
(See above for address)
LEAD ATTORNEY

ATTORNEY TO BE NOTICED

Thomas P Liddy
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Thomas Galvin
as a member of the Maricopa County Board of Supervisors

represented by **Emily Mae Craiger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph James Branco
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Eugene LaRue
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Karen J Hartman-Tellez
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Thomas P Liddy
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Steve Gallardo
as a member of the Maricopa County Board of Supervisors

represented by **Emily Mae Craiger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph James Branco
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Eugene LaRue
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Karen J Hartman-Tellez
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Thomas P Liddy
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Rex Scott
as a member of the Pima County Board of Supervisors

represented by **Daniel S Jurkowitz**
Pima County Attorneys Office
32 N Stone Ave., Ste. 2100
Tucson, AZ 85701
520-740-5750
Fax: 520-740-5600
Email: Daniel.Jurkowitz@pcao.pima.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Matt Heinz
as a member of the Pima County Board of Supervisors

represented by **Daniel S Jurkowitz**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Sharon Bronson
as a member of the Pima County Board of Supervisors

represented by **Daniel S Jurkowitz**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Steve Christy
as a member of the Pima County Board of Supervisors

represented by **Daniel S Jurkowitz**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Adelita Grijalva
as a member of the Pima County Board of Supervisors

represented by **Daniel S Jurkowitz**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Maricopa County Board of Supervisors

represented by **Emily Mae Craiger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph James Branco
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Eugene LaRue
(See above for address)

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Karen J Hartman-Tellez
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Thomas P Liddy
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Amicus

Arizona Republican Party represented by **Michael Kielsky**
Udall Shumway PLC
1138 N Alma School Rd., Ste. 101
Mesa, AZ 85201-6695
480-461-5309
Fax: 480-833-9392
Email: mk@udallshumway.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
04/22/2022	1	COMPLAINT. Filing fee received: $ 402.00, receipt number AAZDC-20590502 filed by Mark Finchem, Kari Lake. (Parker, Andrew) (Attachments: # 1 Civil Cover Sheet)(JAM) (Entered: 04/25/2022)
04/22/2022	2	Filing fee paid, receipt number AAZDC-20590502. This case has been assigned to the Honorable Deborah M Fine. All future pleadings or documents should bear the correct case number: CV-22-677-PHX-DMF. Magistrate Election form attached. (JAM) (Entered: 04/25/2022)
05/04/2022	3	AMENDED COMPLAINT against All Defendants filed by Mark Finchem, Kari Lake. (Parker, Andrew) (Entered: 05/04/2022)
05/04/2022	4	NOTICE of Filing Amended Pleading pursuant to LRCiv 15.1(b) by Mark Finchem, Kari Lake . (Parker, Andrew) (Entered: 05/04/2022)
05/10/2022	6	SUMMONS Submitted by Mark Finchem, Kari Lake. (Parker, Andrew) (Entered: 05/10/2022)
05/10/2022	8	Party Elects Assignment of Case to District Judge Jurisdiction. This is a TEXT ENTRY ONLY. There is no PDF document associated with this entry. (MAP) (Entered: 05/11/2022)
05/11/2022	7	Summons Issued as to Sharon Bronson, Steve Christy, Steve Gallardo, Thomas Galvin, Bill Gates, Adelita Grijalva, Matt Heinz, Clint Hickman, Katie Hobbs, Rex Scott, Jack Sellers. (BAS). *** IMPORTANT: When printing the summons, select "Document and stamps" or "Document and comments" for the seal to appear on the document. (Entered: 05/11/2022)
05/11/2022	9	MINUTE ORDER: Pursuant to Local Rule 3.7(b), a request has been received for a random reassignment of this case to a District Judge. FURTHER ORDERED Case

		reassigned by random draw to Judge John J Tuchi. All further pleadings/papers should now list the following COMPLETE case number: CV-22-00677-PHX-PHX-JJT. This is a TEXT ENTRY ONLY. There is no PDF document associated with this entry. (MAP) (Entered: 05/11/2022)
05/12/2022	10	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Sharon Bronson on 05/11/2022. (Parker, Andrew) (Entered: 05/12/2022)
05/12/2022	11	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Steve Christy on 05/11/2022. (Parker, Andrew) (Entered: 05/12/2022)
05/12/2022	12	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Adelita Grijalva on 05/11/2022. (Parker, Andrew) (Entered: 05/12/2022)
05/12/2022	13	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Matt Heinz on 05/11/2022. (Parker, Andrew) (Entered: 05/12/2022)
05/12/2022	14	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Rex Scott on 05/11/2022. (Parker, Andrew) (Entered: 05/12/2022)
05/12/2022	15	ORDER: IT IS ORDERED that motions to dismiss pursuant to Fed. R. Civ. P. 12(b) and motions to strike pursuant to Fed. R. Civ. P. 12(f) are discouraged if the defect that would be the subject of the motion can be cured by filing an amended pleading. IT IS FURTHER ORDERED that Plaintiff shall serve a copy of this Order onDefendants. (See attached Order). Signed by Judge John J Tuchi on 5/12/2022. (JAMA) (Entered: 05/12/2022)
05/12/2022	16	ORDER: IT IS HEREBY ORDERED directing the Clerk of Court to terminate any or all Defendants in this matter, without further notice, that have not been served within the time required by Fed. R. Civ. P. 4(m) on July 22, 2022. (See attached Order). Signed by Judge John J Tuchi on 5/12/2022. (JAMA) (Entered: 05/12/2022)
05/13/2022	17	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Bill Gates on 05/11/2022. (Parker, Andrew) (Entered: 05/13/2022)
05/13/2022	18	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Clint Hickman on 05/11/2022. (Parker, Andrew) (Entered: 05/13/2022)
05/13/2022	19	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Jack Sellers on 05/11/2022. (Parker, Andrew) (Entered: 05/13/2022)
05/13/2022	20	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Kathleen Hobbs on 05/11/2022. (Parker, Andrew) (Entered: 05/13/2022)
05/13/2022	21	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Steve Gallardo on 05/11/2022. (Parker, Andrew) (Entered: 05/13/2022)
05/13/2022	22	SERVICE EXECUTED filed by Mark Finchem, Kari Lake: Proof of Service re: Summons, Complaint, Civil Cover Sheet, Notice of Filing Amended Complaint, Amended Complaint upon Thomas Galvin on 05/11/2022. (Parker, Andrew) (Entered: 05/13/2022)

05/16/2022		Remark: Pro hac vice motion(s) granted for Kurt B Olsen on behalf of Plaintiffs Mark Finchem, Kari Lake. This is a TEXT ENTRY ONLY. There is no PDF document associated with this entry. (BAS) (Entered: 05/16/2022)
05/18/2022		Remark: Out of state attorney Alan M Dershowitz terminated as counsel of record for noncompliance with admission procedures; party or parties represented by other admitted counsel. This is a TEXT ENTRY ONLY. There is no PDF document associated with this entry. (BAS) (Entered: 05/18/2022)
05/27/2022	23	NOTICE of Appearance by Roopali H Desai on behalf of Katie Hobbs. (Desai, Roopali) (Entered: 05/27/2022)
05/31/2022	24	STIPULATION FOR EXTENSION OF TIME TO ANSWER COMPLAINT re: 3 Amended Complaint *First Request* by Maricopa County Board of Supervisors. (Attachments: # 1 Proposed Order Proposed Order)(Craiger, Emily) (Entered: 05/31/2022)
06/01/2022	25	NOTICE of Appearance by Emily Mae Craiger on behalf of Maricopa County Board of Supervisors. (Craiger, Emily) (Entered: 06/01/2022)
06/06/2022	26	ORDER: IT IS HEREBY ORDERED granting the parties' Joint Stipulation for Extension of Time for Defendants to File Responsive Pleading (Doc. 24). IT IS FURTHER ORDERED extending the deadline for Defendants to file an Answer or otherwise respond to Plaintiffs' First Amended Complaint (Doc. 3) to June 8, 2022. Signed by Judge John J Tuchi on 6/6/2022. (JAMA) (Entered: 06/06/2022)
06/07/2022	27	*MOTION to Dismiss for Failure to State a Claim *//Maricopa County Defendants' Motion To Dismiss Plaintiffs First Amended Complaint* by Steve Gallardo, Thomas Galvin, Bill Gates, Clint Hickman, Maricopa County Board of Supervisors, Jack Sellers. (Craiger, Emily) *Modified to correct event, attorney noticed on 6/8/2022 (LAD). (Entered: 06/07/2022)
06/07/2022	28	*MOTION for Leave to File Excess Pages for Motion *To Dismiss Plaintiffs First Amended Complaint (Doc 27)* by Maricopa County Board of Supervisors. (Craiger, Emily) *Modified docket text to remove additional filers on 6/8/2022. (SMH) (Entered: 06/07/2022)
06/07/2022	29	MOTION Judicial Notice re: 27 MOTION to Dismiss Case *//Maricopa County Defendants' Motion To Dismiss Plaintiffs First Amended Complaint* by Steve Gallardo, Thomas Galvin, Bill Gates, Clint Hickman, Maricopa County Board of Supervisors, Jack Sellers. (Attachments: # 1 Attachment A, # 2 Exhibit 1, # 3 Exhibit 2, # 4 Exhibit 3, # 5 Exhibit 4, # 6 Exhibit 5, # 7 Exhibit 6, # 8 Exhibit 7, # 9 Exhibit 8, # 10 Exhibit 9, # 11 Exhibit 10, # 12 Exhibit 11, # 13 Exhibit 12, # 14 Exhibit 13, # 15 Exhibit 14, # 16 Exhibit 15, # 17 Exhibit 16, # 18 Exhibit 17)(Craiger, Emily) (Entered: 06/07/2022)
06/07/2022	30	NOTICE re: Certificate of Good Faith Consulatation by Steve Gallardo, Thomas Galvin, Bill Gates, Clint Hickman, Maricopa County Board of Supervisors, Jack Sellers re: 27 MOTION to Dismiss Case *//Maricopa County Defendants' Motion To Dismiss Plaintiffs First Amended Complaint* . (Attachments: # 1 Exhibit 1)(Craiger, Emily) (Entered: 06/07/2022)
06/08/2022	31	*Joinder re: 27 MOTION to Dismiss Case for Failure to State a Claim by Sharon Bronson, Steve Christy, Adelita Grijalva, Matt Heinz, Rex Scott. (Jurkowitz, Daniel) *Modified to correct event type on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	32	MOTION for Leave to File Excess Pages for Motion and Memorandum *for Preliminary Injunction* by Mark Finchem, Kari Lake. (Attachments: # 1 Proposed Order)(Parker, Andrew) (Entered: 06/08/2022)

06/08/2022	33	LODGED Proposed Plaintiffs' Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion re: 32 MOTION for Leave to File Excess Pages for Motion and Memorandum *for Preliminary Injunction*. Document to be filed by Clerk if Motion or Stipulation for Leave to File or Amend is granted. Filed by Mark Finchem, Kari Lake. (Parker, Andrew) (Entered: 06/08/2022)
06/08/2022	34	Additional Attachments to Main Document re: 33 Lodged Proposed Document, by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) (Entered: 06/08/2022)
06/08/2022	35	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Declaration of Benjamin R. Cotton* by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) *Modified to correct docket text on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	36	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Exhibits A-G to Cotton Declaration* by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) *Modified to correct docket text and linkage on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	37	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Exhibits H-J to Cotton Declaration* by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) *Modified to correct docket text and linkage on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	38	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Declaration of Walter C. Daugherity* by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) *Modified to correct docket text on 6/10/2022 (SMH). (Entered: 06/08/2022)
06/08/2022	39	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Declaration of Douglas Logan* by Plaintiffs Mark Finchem, Kari Lake. (Attachments: # 1 Exhibit A-E)(Parker, Andrew) *Modified to correct docket text on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	40	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Declaration of John R. Mills* by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) *Modified to correct docket text on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	41	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Declaration of Shawn A. Smith* by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) *Modified to correct docket text on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	42	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion by Plaintiffs Mark Finchem, Kari Lake. (Attachments: # 1 Exhibit A-G)(Parker, Andrew) *Modified to correct docket text on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	43	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Exhibit H to Parker Declaration* by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) *Modified to correct docket text and linkage on 6/10/2022. (SMH) (Entered: 06/08/2022)
06/08/2022	44	*Additional Attachments to Main Document re: 33 Motion for Preliminary Injunction and Memorandum of Points and Authorities in Support of Motion *Exhibit I and J to Parker Declaration* by Plaintiffs Mark Finchem, Kari Lake. (Parker, Andrew) *Modified to correct docket text and linkage on 6/10/2022. (SMH) (Entered: 06/08/2022)

06/08/2022		Remark: Pro hac vice motion(s) granted for Christine Bass on behalf of Defendant Katie Hobbs. This is a TEXT ENTRY ONLY. There is no PDF document associated with this entry. (WLP) (Entered: 06/08/2022)
06/08/2022	45	MOTION to Dismiss for Failure to State a Claim *Arizona Secretary of State's Motion to Dismiss First Amended Complaint* by Katie Hobbs. (Desai, Roopali) (Entered: 06/08/2022)
06/08/2022	46	NOTICE re: Certification of Conferral by Katie Hobbs re: 45 MOTION to Dismiss for Failure to State a Claim *Arizona Secretary of State's Motion to Dismiss First Amended Complaint* . (Desai, Roopali) (Entered: 06/08/2022)
06/14/2022	47	MOTION for Leave to File Amicus Brief by Arizona Republican Party. (Attachments: # 1 Proposed Order)(Kielsky, Michael) (Entered: 06/14/2022)
06/14/2022	48	LODGED Proposed Amicus Brief re: 47 MOTION for Leave to File Amicus Brief . Document to be filed by Clerk if Motion or Stipulation for Leave to File or Amend is granted. Filed by Arizona Republican Party. (Kielsky, Michael) (Entered: 06/14/2022)

PACER Service Center

Transaction Receipt

06/14/2022 08:11:07

PACER Login:		**Client Code:**	
Description:	Docket Report	**Search Criteria:**	2:22-cv-00677-JJT
Billable Pages:	10	**Cost:**	1.00

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

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Kari Lake and Mark Finchem,

Plaintiffs,

v.

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

Defendants.

No. ________________

COMPLAINT

(Jury Trial Demanded)

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

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

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

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

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

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

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

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

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

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

I. INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I. PARTIES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

II. JURISDICTION AND VENUE

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

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

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

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

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

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

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

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

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

III. FACTUAL ALLEGATIONS

A. Background

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

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

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

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

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

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

[3] 52 U.S.C. § 20901 *et seq*.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

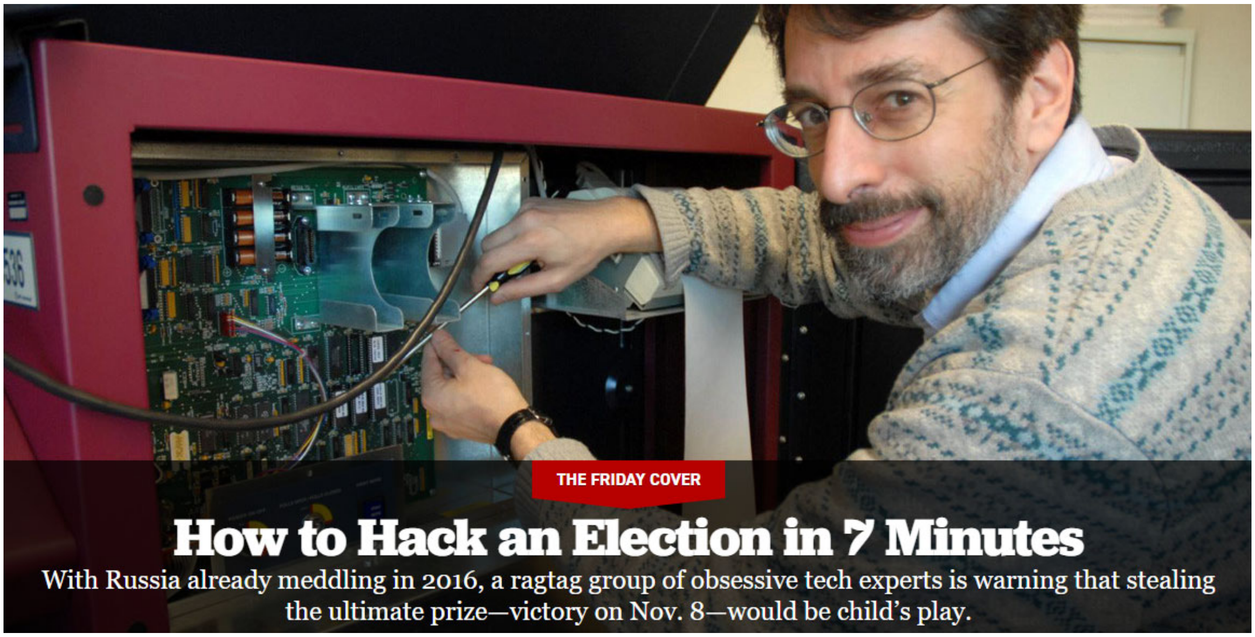
76. In 2015 the Brennan Center for Justice issued a report listing two and a half-pages of instances of issues with voting machines, including a 2014 investigation which found "voters in Virginia Beach observed that when they selected one candidate, the machine would register

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

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

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

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



THE FRIDAY COVER

How to Hack an Election in 7 Minutes

With Russia already meddling in 2016, a ragtag group of obsessive tech experts is warning that stealing the ultimate prize—victory on Nov. 8—would be child's play.

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

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

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

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

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

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

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

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

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

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

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

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

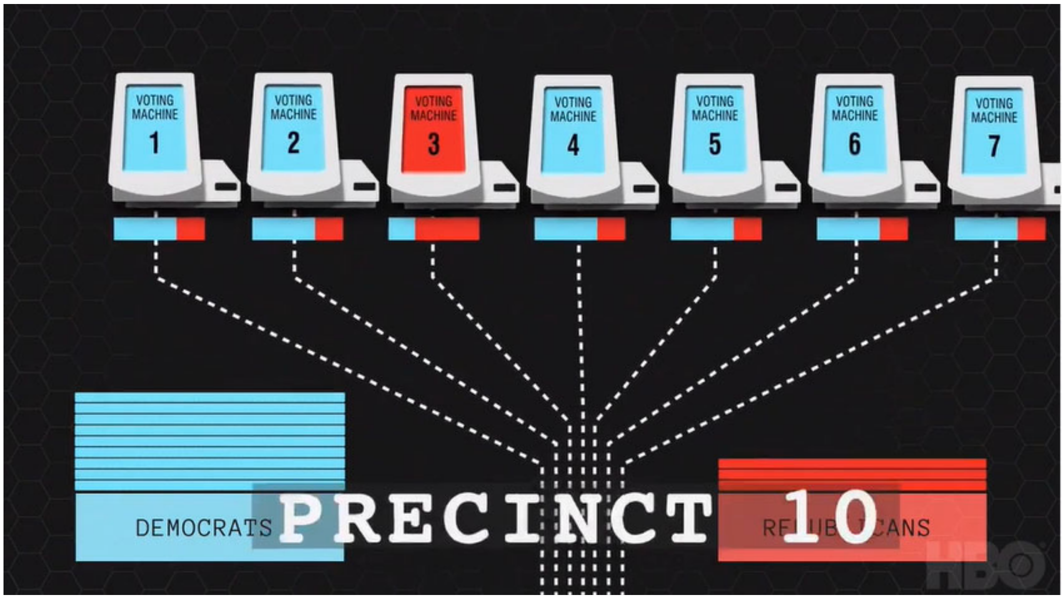
the internet because they didn’t know differently.”[12] The Associated Press reported that the vast majority of 10,000 election jurisdictions nationwide were still using Windows 7 or older operating systems to create ballots, program voting machines, tally votes, and report counts, which was a problem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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

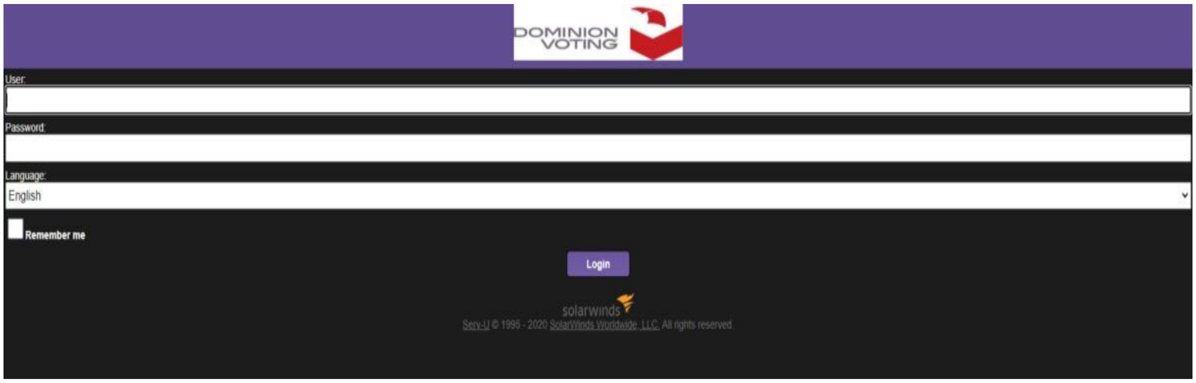
[25] Isabel van Brugen, *Dominion Voting Machines Were Updated Before Election, Georgia Official Confirms*, The Epoch Times (Dec. 4, 2020) (https://www.theepochtimes.com/dominion-voting-machines-were-updated-before-election-georgia-official-confirms_3604668.html).

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

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

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

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



English

□ Remember me

Serv-U © 1995 - 2020 SolarWinds Worldwide, LLC. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

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

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

[28] M.D. Kittle, *Emails: Green Bay's 'Hidden' Election Networks*, Wisconsin Spotlight (Mar. 21, 2021) (https://wisconsinspotlight.com/emails-green-bays-hidden-election-networks/).

[29] Natasha Truak and Amanda Macias, *Biden administration slaps new sanctions on Russia for cyberattacks, election interference*, CNBC (Apr. 16, 2021) (https://www.cnbc.com/2021/04/15/biden-administration-sanctions-russia-for-cyber-attacks-election-interference.html).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Though a uniform chain of custody, ballot boxes are conveyed to a precinct level counting location while still sealed.
- With party representatives, ballot boxes are unsealed, one at a time, and ballots are removed and counted in batches of 100, then returned to the ballot box. When all ballots in a ballot box have been counted, the box is resealed, with a copy of the batch tally sheets left inside the box, and the batch tally sheets carried to the tally center with a uniform chain of custody.
- Ballots are counted, one at a time, by three independent counters, who each produce a tally sheet that is compared to the other tally sheets at the completion of each batch.
- At the tally center, two independent talliers add the counts from the batch sheets, and their results are compared to ensure accuracy.
- Vote counting from paper ballots is conducted in full view of multiple, recording, streaming cameras that ensure a) no ballot is ever touched or accessible to anyone off-camera or removed from view between acceptance of a cast ballot and completion of counting, b) all ballots, while being counted are in full view of a camera and are readable on the video, and c) batch tally sheets and precinct tally sheets are in full view of a camera while being filled out and are readable on the video.
- Each cast ballot, from the time of receipt by a sworn official from a verified, eligible elector, remains on video through the completion of precinct counting and reporting.
- The video be live-streamed for public access and archived for use as an auditable record, with public access to replay a copy of that auditable record.

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

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

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

J. Past and Threatened Conduct of Defendant Hobbs

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

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

A.R.S. § 16-452 (A).

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

A.R.S. § 16-452 (D).

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

- "Be suitably designed for the purpose used and be of durable construction, and may be used safely, efficiently and accurately in the conduct of elections and counting ballots…"

- "When properly operated, record correctly and count accurately every vote cast…" and

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

A.R.S. § 16-446 (B).

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

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

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

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

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

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

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

A.R.S. § 11-251.

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

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

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

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

L. Imminent Injury

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

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

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

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

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

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

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

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

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

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

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

IV. CLAIMS

COUNT I: VIOLATION OF DUE PROCESS

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

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

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

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

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

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

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

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

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

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

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

COUNT II: VIOLATION OF EQUAL PROTECTION

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

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

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

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

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

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

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

COUNT III: VIOLATION OF FUNDAMENTAL RIGHT TO VOTE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COUNT V: VIOLATION OF A.R.S. § 11-251

(Against Maricopa Defendants and Pima Defendants)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

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

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

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

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

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

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

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

DEMAND FOR JURY TRIAL

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

DATED: April 22, 2022.

PARKER DANIELS KIBORT LLC

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

OLSEN LAW, P.C.

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

Counsel for Plaintiffs Kari Lake
and Mark Finchem

ALAN DERSHOWITZ CONSULTING LLC

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

Of Counsel for Plaintiffs Kari Lake
and Mark Finchem

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): Kari Lake ; Mark Finchem

Defendant(s): Kathleen Hobbs , Arizona Secretary of State; Bill Gates , member of the Maricopa County Board of Supervisors; Clint Hickman , member of the Maricopa County Board of Supervisors; Jack Seller , member of the Maricopa County Board of Supervisors; Thomas Galvin , member of the Maricopa County Board of Supervisors; Steve Gallardo , member of the Maricopa County Board of Supervisors; Rex Scott , member of the Pima County Board of Supervisors; Matt Heinz , member of the Pima County Board of Supervisors; Sharon Bronson , member of the Pima County Board of Supervisors; Steve Christy , member of the Pima County Board of Supervisors; Adelita Grijalva , member of the Pima County Board of Supervisors

County of Residence: Maricopa

County Where Claim For Relief Arose: Maricopa

County of Residence: Maricopa

Plaintiff's Atty(s):

Defendant's Atty(s):

Andrew D Parker , Attorney
Parker Daniels Kibort LLC
123 N. Third Street, Suite 888
Minneapolis, Minnesota 55401
6123554100

II. Basis of Jurisdiction: **3. Federal Question (U.S. not a party)**

III. Citizenship of Principal Parties **(Diversity Cases Only)**
Plaintiff:- **N/A**
Defendant:- **N/A**

IV. Origin : **1. Original Proceeding**

V. Nature of Suit: **441 Voting**

VI.Cause of Action: **42 U.S.C. § 1983**

VII. Requested in Complaint
Class Action: **No**
Dollar Demand:
Jury Demand: **Yes**

VIII. This case **is not related** to another case.

Signature: /s/ Andrew D. Parker

Date: 04/22/2022

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014