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

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. **Electronic Voting System Manufacturers Not Reliable.**

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. **Hand Voting and Counting With Paper Ballots Is Practical.**

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. Plaintiffs Are Likely to Succeed on the Merits.

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. <u>Plaintiffs Will Suffer Irreparable Harm Absent Preliminary Relief.</u>

"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. <u>The Balance of Equities Favors an Injunction.</u>

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. **The Requested Injunction Is in the Public Interest.**

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